



Benutzerhandbuch

Dr.Web Agent
Version 6.0.3
Benutzerhandbuch
02.11.2011

Doctor Web, Hauptsitz Russland
Tretja ul. Jamskogo polja 2, Gebäude 12A
125124 Moskau
Russische Föderation

Website: www.drweb.com
Telefon: +7 (495) 789-45-87

Nähere Informationen zu den regionalen Vertretungen und Büros finden Sie auf unserer Website

Doctor Web

Doctor Web ist ein russischer Anbieter hauseigener IT-Sicherheitslösungen.

Doctor Web bietet effektive Antivirus- und Antispam-Lösungen sowohl für staatliche Einrichtungen und große Unternehmen als auch für private Benutzer.

Die Antivirensoftware von Dr.Web wird seit 1992 entwickelt. Die Antivirus-Lösungen zeigen immer wieder hervorragende Leistungen bei Entdeckung von Malware und entsprechen den weltweiten Sicherheitsnormen.

Zertifikate und Auszeichnungen sowie umfangreiche Geographie der Benutzer zeugen vom besonderen Vertrauen der Kunden in unsere Produkte.

Wir danken den Benutzern für Unterstützung der Lösungen von Dr.Web-Familie!



Inhaltsverzeichnis







Kapitel 1. Einleitung

1.1. Symbole und Abkürzungen

Symbole

In diesem Benutzerhandbuch werden die Bezeichnungen, die in Tabelle 1 angeführt sind, verwendet.

Tabelle 1. Symbole

Bezeichnung	Erläuterung
Achten Sie, dass	Wichtige Bemerkung oder Hinweis.
Achtung	Warnung vor möglichen Fehlersituationen sowie wichtigen Momenten, die besonderer Rücksicht bedürfen.
Dr.Web Agent	Produkt- und Komponentennamen von **Dr.Web**.
Antivirus-Netzwerk	Ein Begriff tritt als Definition auf.
<IP-address>	Felder zum Ersatz von Funktionsnamen durch t atsächliche Werte.
Übernehmen	Namen der Tasten, Fenster, Menüpunkte und sonstigen Bestandteile der Benutzeroberfläche.
CTRL	Bezeichnungen der Tastaturtasten.
`C:\Windows\`	Namen der Dateien und Ordner, Ausschnitte des Programmcodes.
Anhang A	Querverweise zu Dokumentkapiteln oder Hyperlinks zu externen Ressourcen.



Abkürzungen

Im Text des Handbuches werden folgende Abkürzungen ohne Erläuterung verwendet:

- FDD – Floppy Disk Drive (Diskette – transportabler magnetischer Datenträger),
- GUI – Graphical User Interface (grafische Benutzeroberfläche), GUI-Programmversion - eine Version, die GUI-Mittel benutzt,
- UAC – User Account Control (Benutzerkontensteuerung - Komponente von Microsoft Windows. Die UAC fordert Bestätigung der Aktionen, die Administratorrechte bedürfen, an, um den Schutz vor Missbrauch des Computers zu gewährleisten),
- URL – Uniform Resource Locator (Einheitlicher Quellenanzeiger – die im World Wide Web verwendete standartisierte Darstellung von Internetadressen),
- **GAS Dr.Web** – **Globales Aktualisierungssystem von Dr. Web,**
- OS – Betriebssystem,
- SW – Software.

1.2. Dr.Web® Antivirus Enterprise Security Suite

Dr.Web Enterprise Security Suite dient der Einrichtung und Verwaltung eines einheitlich und zuverlässig wirkenden, komplexen Virenschutzes für Computer Ihres Unternehmens.

Geschützte Computer werden in ein Antivirus-Netzwerk vereinigt, das vom Administrator über einen **Enterprise Server** verwaltet wird. Der Schutz von Computern der Mitarbeiter ist automatisiert und wird zentral verwaltet, was ein zuverlässiges Sicherheitsniveau beim minimalen Eingreifen seitens Personals gewährleistet.

Dr.Web Enterprise Security Suite löst folgende Aufgaben:

- Zentralisierte (ohne dass direkter Zugriff des Personals benötigt wird) Installation der Antivirus-Pakete auf den geschützten Computern,
- Zentralisierte Parametereinstellung von Antivirus-Paketen auf den geschützten Computern,
- Zentralisierte Aktualisierung der Virendatenbanken und der Software auf den geschützten Computern,
- Monitoring von Virenereignissen sowie vom Zustand der Antivirus-Pakete und des Betriebssystems auf allen geschützten Computern.

Auf den geschützten Computern wird **Dr.Web Agent** installiert. Diese Komponente gewährleistet die Verwaltung des Computerschutzes und steht in Verbindung mit dem **Enterprise Server**, über den die Antivirus-Programme und deren Komponenten aktualisiert sowie Grundparameter von der auf den Computern installierten Antivirus-Software eingestellt werden.



Auf den Computern mit installiertem **Dr.Web Agenten** muss keine andere Antivirus-Software installiert werden, eingeschlossen von anderen Versionen der **Dr.Web** Software.

Einstellungen, die für Benutzer zugänglich sind, werden im Abschnitt Dr.Web Agent verwalten beschrieben.



Kapitel 2. Komponente Dr.Web Agent

2.1. Grundfunktionen und Parameter des Dr.Web Agenten

Dem Schutz von Computern vor Virenbedrohungen und Spam dienen Programme, die zum Antivirus-Paket **Dr.Web Enterprise Security Suite** gehören.

Die Verwaltung des Computerschutzes und Verbindung zum **Enterprise Server** erfolgt mit Hilfe des **Dr.Web Enterprise Security Suite Agenten** (im weiteren **Dr.Web Agent**).

Dr.Web Agent erfüllt folgende Funktionen:

- installiert, aktualisiert und stellt das **Dr.Web** Antivirus-Paket ein, startet den Scanvorgang sowie führt andere Aufgaben aus, die vom **Enterprise Server** erstellt werden;
- lässt die Komponenten des **Dr.Web** Antivirus-Pakets über spezielle Benutzeroberfläche aufrufen;
- übergibt die Ergebnisse der Aufgabenausführung dem **Enterprise Server**;
- übergibt dem **Enterprise Server** die Nachrichten über das Entstehen der voreingestellten Ereignisse in der Funktion des Antivirus-Pakets.

Der Benutzer kann folgende Aktionen mit Hilfe des Dr.Web Agenten ausführen:

- den Zeitplan zur Virenprüfung (Scannen) des Computers einstellen;
- Scannen des Computers bei Bedarf starten;
- Einstellungen einzelner Komponenten vom **Dr.Web** Programmkomplex, darunter auch manche Einstellungen des **Agenten** selbst, ändern;



- Statistik der Virenereignisse auf dem Computer sowie andere Informationen über den **Dr.Web** Programmkomplex anschauen.



Zur Änderung von Einstellungen des **Agenten** und der Komplex-Komponenten muss der Benutzer entsprechende Rechte besitzen. Weitere Information hierzu finden Sie in den Beschreibungen der Einstellungen für bestimmte Komponenten.

2.2. Systemanforderungen



Auf Workstations des Antivirus-Netzwerkes, das mit Hilfe von **Dr.Web** verwaltet wird, muss keine andere Antivirus-Software verwendet werden (einschließlich anderer Versionen von **Dr.Web** Antivirus-Software).

Zur Funktion des Dr.Web Agenten und des vollständigen Antivirus-Pakets wird folgendes erforderlich sein:

1. Minimale Anforderungen:
   - Prozessor Intel® Pentium® IV 1.6 GHz;
   - Hauptspeicher 512 MB.
2. Empfohlene Anforderungen:
   - Prozessor Intel® Pentium® IV 2.4 GHz oder höher;
   - Hauptspeicher mindestens 1 GB.
3. Freier Speicherplatz auf der Festplatte: mindestens 182 MB für ausführbare Dateien + zusätzlich für Funktionsprotokolle und temporäre Dateien.
4. Betriebssysteme (s. Anhang B. Vollständige Liste von unterstützten Betriebssystemen):

   a) OS Microsoft® Windows® 98, OS Windows Me, OS Windows NT4 (SP6) oder höher. Je nach Betriebssystem können folgende Komponenten dabei installiert werden:



Komponente	Betriebssystem
SpIDer Gate, **SelfPROtect** und **Office Kontrolle**	Windows 2000 (SP4) oder höher.
FireWall	Windows 2000 (SP4 + Update Rollup 1) oder höher.
SpIDer Guard NT4	• Windows 98, • Windows ME, • Windows NT4 (SP6a), • Windows 2000 mit SP4 ohne Update Rollup1, • Windows XP ohne SP sowie mit SP1, • Windows 2003 ohne SP.
SpIDer Guard G3	• Windows 2000 mit SP4 und Update Rollup1, • Windows XP mit SP2 oder neuer, • Windows 2003 mit SP1 oder neuer, • Windows Vista oder neuer.
SpIDer Mail NT4	• Windows 98, • Windows NT4 mit SP6a.
SpIDer Mail	Unter sämtlichen unterstützten Betriebssystemen, die neuer als die für Version **SpIDer Mail NT4**.
Dr.Web Browser-Plugin für Outlook	Windows 2000 mit SP4 oder neuer.

b) Microsoft® Windows Mobile®;

c) Novell® NetWare®;

d) Mac OS® X;

e) Betriebssysteme der UNIX®-Familie: OS Linux®, OS FreeBSD® oder OS Solaris™.



Informationen zur **Agenten**-Funktionalität unter Windows Mobile und Novell NetWare finden Sie in den Benutzerhandbüchern **Dr.Web Agent für Windows Mobile** und **Dr.Web Agent für Novell NetWare**.

5. Für das anzuschließende Modul **Dr.Web für Outlook** ist installierter Microsoft Outlook Client von MS Office erforderlich:
   - Outlook 2000 (Outlook 9),
   - Outlook 2002 (Outlook 10 oder Outlook XP),
   - Office Outlook 2003 (Outlook 11),
   - Office Outlook 2007,
   - Office Outlook 2010.
6. Zur korrekten Funktion der Kontexthilfe **Dr.Web Agent für Windows** ist Windows® Internet Explorer® 6.0 oder höher erforderlich.

2.3. Antivirus-Software installieren und deinstallieren

2.3.1. Installation des Dr.Web Agenten

Vor Beginn der Installation von Antivirus-Software achten Sie auf den Abschnitt Systemanforderungen.



Für die Installation des **Dr.Web Agenten** benötigt der Benutzer die Administratorrechte.

Installation und Deinstallation des **Dr.Web Agenten** und des Antivirus-Pakets kann auf zwei Weisen ausgeführt werden:



1. Entfernt - auf dem **Server** über Netzwerk. Die Installation wird vom Administrator des Antivirus-Netzwerkes ausgeführt. Das Eingreifen seitens des Benutzers ist nicht erforderlich (ausführliche Information zur Errichtung einer Antivirus-Station und entfernten Installation der Antivirus-Software finden Sie im Administratorhandbuch **Dr.Web Enterprise Security Suite Antivirus).**



Entfernte Installation der **Dr.Web Agenten** ist nur für Workstations, die unter Windows NT4 oder neuer funktionieren, möglich.

Zur entfernten Software-Installation sind die Administratorrechte für Workstation erforderlich.

2. Lokal - direkt auf dem Benutzercomputer. Die Installation kann sowohl vom Administrator als auch vom Benutzer ausgeführt werden. Dabei kann die Installation mit Hilfe folgender Komponenten erfolgen:
   - Installationspaket `esinst.exe`.
   - Netzwerkinstallations-Assistent **Агента** `drwinst.exe`.

   Nachfolgend finden Sie die Beschreibung der lokalen Installation und Deinstallation von Antivirus-Software.

2.3.1.1. Installation des Dr.Web Agenten mit Hilfe des Installationspakets

Falls auf einer Workstation die Antivirus-Software schon installiert ist, versucht das Installationsprogramm vor Installationsbeginn diese zu löschen. Beim Fehlversuch müssen Sie die auf der Workstation verwendete Antivirus-Software selbstständig löschen.

Um den Agenten und das Antivirus-Paket auf der Workstation zu installieren:

1. Laden die Installationsdatei des **Agenten** herunter. Dafür klicken Sie auf den Link, den Sie vom Administrator des Antivirus-Netzwerkes erhalten haben.



2. Starten Sie die heruntergeladene `esinst.exe` Datei. Dabei öffnet sich das Fenster des Installationswizards von **Dr.Web** Antivirus.
3. Vor Beginn der Installation bittet der Installationswizard zu bestätigen, dass keine Antivirus-Programme auf dem Computer installiert sind. Stellen Sie sicher, dass keine andere Antivirus-Software (darunter auch andere Versionen der Antivirus-Software von **Dr.Web**) auf dem Computer benutzt wird. Danach setzen Sie ein Häkchen bei **Auf meinem Computer gibt es keine andere Antivirus-Software** und klicken Sie auf **Weiter.**
4. Im nächsten Fenster wird es angeboten, den Installationstyp zu wählen:
   - **Schnellinstallation (empfehlenswert)** - die einfachste Installationsvariante. Sämtliche Parameter werden automatisch festgelegt. Gehen Sie direkt weiter zu Schritt **9**.
   - **Benutzerdefinierte Installation** - Installationsvariante, bei der Sie die Komponenten der auf dem Computer zu installierenden Antivirus-Software auswählen können.
   - **Administrative Installation** - die meist vollständige Installationsvariante. Dieser Installationstyp lässt sämtliche Parameter der Installation sowie der zu installierenden Antivirus-Software festlegen/ändern.
5. Bei Installationsvarianten **Benutzerdefinierte Installation** und **Administrative Installation** können Sie im nächsten Fenster die Komponenten des **Dr.Web** Antivirus-Pakets auswählen. Setzen Sie Häkchen bei den Komponenten, die Sie auf Ihrem Computer installieren möchten.

   Im Abschnitt **Pfad des Installationsordners** können Sie den Ordner festlegen, in dem die Antivirus-Software installiert wird. Standardmäßig ist es der Ordner `Dr.Web Enterprise Suite`, der sich im `Program files` Ordner auf der Systemplatte befindet. Zur Änderung des Installationspfads klicken Sie auf **Durchsuchen** und geben Sie den erforderlichen Pfad an.

   Klicken Sie auf **Weiter**.



Bei der Installationsvariante **Benutzerdefinierte Installation** gehen Sie direkt weiter zu Schritt **9**.

6. Bei der Installationsvariante **Administrative Installation:** im nächsten Fenster legen Sie die Einstellungen des **Netzwerkinstallers** fest:

   - Im Feld **Dr.Web Enterprise Server** wird die Netzwerkadresse des **Enterprise Servers** angegeben, von dem **Agent** und Antivirus-Paket installiert werden. Wenn Sie beim Starten des Installationsprogramms die Adresse des **Servers** angegeben haben, wird diese Adresse automatisch ins genannte Feld eingetragen.



Bei Installation des **Agenten** mit Hilfe des Installationsassistenten, geschaffen im **Verwaltungscenter**, wird das Feld **Dr.Web Enterprise Server** automatisch ausgefüllt.

Falls die **Server**-Adresse Ihnen unbekannt ist, klicken Sie auf den **Suche**-Knopf. Dabei offnet sich ein Fenster zur Suche von aktiven **Enterprise Server** des Netzwerkes. Legen Sie erforderliche Parameter (im Format *<Servername>*@*<IP-Adresse>*/*<Netzwerkpräfix>*: *<Port>*) fest und klicken Sie auf den **Suche**-Knopf. Aus der Liste der gefundenen **Server** wählen Sie den Server aus, von dem die Antivirus-Software installiert wird, und klicken Sie auf **OK**.

   - Im Feld **Dr.Web Enterprise Server öffentlicher Schlüssel** wird der vollständige Pfad des öffentlichen Schlüssels (`drwcsd.pub`) angegeben, der sich auf Ihrem Computer befindet (wird das Installationsprogramm vom **Server** über Netzwerk gestartet, so wird der Schlüssel in die temporären Dateien des Betriebssystems kopiert und nach der Installation in den Installationsordner übertragen).
   - Im Abschnitt **Komprimierung beim Herunterladen verwenden** wählen Sie gewünschte Variante zum Komprimieren des Verkehrs: **Ja** - Komprimierung verwenden, **Nein** - nicht verwenden, **Möglich** - die Verwendung der Komprimierung hängt von **Server**-Einstellungen ab.

- Das Häkchen bei **Dr.Web Agenten in die Liste der Ausnahmen von Windows Firewall hinzufügen** bestimmt das Hinzufügen von den vom **Agenten** benutzten Ports und Oberflächen in die Ausnahmenliste vom Netzwerkmonitor des Betriebssystems (außer Windows 2000 oder älter). Es ist empfehlenswert, dieses Häkchen zu setzen. Es hilft, Fehler zu vermeiden, z.B. bei automatischer Aktualisierung von Antivirus-Komponenten und Virendatenbanken.
- Setzen Sie gegebenenfalls ein Häkchen bei **Den Agenten in der Liste der installierten Programme zu registrieren**.

7. Bei der Installationsvariante **Administrative Installation:** im nächsten Fenster legen Sie die Einstellungen des **Agenten** fest:
   - Im Abschnitt **Authorisierung** werden die Parameter für Authorisierung des **Agenten** auf dem **Server** festgelegt. Bei der Auswahl der Variante **Automatisch (standardmäßig)** wird der Zugriffsmodus für Station auf dem **Server** bestimmt. Bei der Variante **Manuell** sind die Authorisierungsparameter der Station festzulegen: **Identifizierer** der Station auf dem **Server** und **Passwort** für den Zugriff darauf. Dabei bekommt die Station den Zugriff, ohne dass die manuelle Bestätigung durch den Administrator auf dem **Server** erforderlich sein wird.

> Bei Installation des **Agenten** mit Hilfe des Installationsassistenten, geschaffen im **Verwaltungscenter**, werden die Felder **Identifizierer** und **Passwort** für Authorisierungsvariante **Manuell** automatisch ausgefüllt.

   - In den Abschnitten **Komprimierung** und **Verschlüsselung** werden entsprechende Modi für den Verkehr zwischen **Server** und **Agenten** festgelegt (weitere Information s. im Punkt **Verwendung von Komprimierung und Verschlüsselung des Verkehrs** in dem Administratorhandbuch zum **Dr.Web Enterprise Security Suite Antivirus**).

Klicken Sie auf **Weiter**.

8. Die Installation des **Agenten** und der Antivirus-Komponenten startet (ohne dass Eingreifen seitens Benutzers erforderlich sein wird).
9. Nach Beendung der Installation benachrichtigt der Installationswizard uber die Notwendigkeit, den Computer neu zu starten. Klicken Sie auf den **Fertig**-Knopf, um den Installationswizard zu beenden.
10. Starten Sie Ihren Computer neu.

2.3.1.2. Installation des Dr.Web Agenten mit Hilfe des Netzwerkinstallations-Assistenten

Wenn der Netzwerkinstallations-Assistent im standardmäßigen Installationsmodus (d.h. ohne `-uninstall` Schlüssel) auf einer Station, wo der **Agent** bereits installiert wurde, gestartet wird, werden dabei keine Aktionen ausgeführt.

Vor Beginn einer neuen Installation ist es erforderlich, den installierten **Agenten** zu löschen.

Die Installation mit dem Netzinstaller ist in zwei Hauptmodi möglich:

1. Im Hintergrundmodus.
2. Im grafischen Modus.



Installation des Dr.Web Agenten mit dem Installer im Hintergrundmodus

Um Antivirus-Software (Dr.Web Agent und Antivirus-Paket) im Hintergrundmodus des Netzinstallers zu installieren:

1. Vom Auf dem Rechner, auf dem die Antivirensoftware installiert wird, starten Sie das `drwinst.exe` Programm, das Sie auf eine der folgenden Weisen finden können:
   - Im Netzwerkinstallationsverzeichnis des **Agenten**. Bei Installation des **Servers** ist es das `Installer` - Unterverzeichnis (per Default versteckte geteilte Ressource) im Installationsverzeichnis des **Servers**. Im Weiteren kann es verschoben werden.
   - Auf der Installationsseite des **Dr.Web Verwaltungscenters**, die auf jedem Rechner mit dem Netzwerkzugriff auf den **Enterprise Server** verfügbar ist, unter:
     `http://`*<Serveradresse>*`:`*<Portnummer>*`/install/`
     wobei als <*Serveradresse*> die IP-Adresse oder der DNS-Name des Rechners, auf dem der **Enterprise Server** installiert ist, anzugeben ist. Als <*Portnummer*> geben Sie die Portnummer `9080` (oder `9081` für https) an.

   Per Default verwendet das ohne Parameter gestartete `drwinst`-Programm den **Multicast**–Modus, um das Netzwerk aufs Vorhandensein der aktiven **Enterprise Server** zu scannen.



Bei Nutzung des **Multicast**–Modus zur Suche der aktiven **Server** wird der **Agent** vom ersten gefundenen **Server** installiert. Wenn dabei der vorhandene `pub`–Schlüssel mit dem Schlüssel des **Servers** nicht übereinstimmt, wird die Installation mit einem Fehler beendet. In diesem Fall geben Sie die explizite Adresse des **Servers** beim Start des Installationsassistenten an (s. unten).

Der `drwinst` Befehl kann auch mit zusätzlichen Parametern ausgeführt werden:

- Wird der **Multicast**-Modus nicht verwendet, so ist es empfehlenswert, den **Server**-Namen (der beim DNS-Dienst registriert wurde) bei der **Agent**-Installation anzuwenden:

`drwinst` *<DNS_Name_des_Enterprise-Servers>*

Dadurch wird die Einstellung des Antivirus-Netzwerkes, die mit Neuinstallation des **Enterprise Servers** auf einem anderen Computer verbunden ist, erleichtert.

- Sie können auch explizite Angabe der **Server**-Adresse benutzen:

`drwinst 192.168.1.3`

- Die Verwendung des `-regagent` Schlüssels lässt den **Agenten** bei der Installation in der Hinzufügen/Entfernen-Programmliste registrieren.
- Um das Installationsprogramm im grafischen Modus zu starten, benutzen Sie den `-interactive` Parameter.



Die komplette Parameterliste des **Netzwerkinstallations-Assistenten** finden Sie im Anhang **H4. Netzwerkinstallations-Assistent** in dem Administratorhandbuch zum **Dr.Web Enterprise Security Suite Antivirus**.

2. Nachdem das Installationsprogramm beendet wird, wird die Software des **Dr.Web Agenten** (aber kein Antivirus-Paket) auf dem Computer installiert.
3. Nach der Bestätigung von Station auf dem **Server** (falls es durch **Server**-Einstellungen vorgesehen ist) wird das Antivirus-Paket automatisch installiert.
4. Starten Sie Ihren Computer nach Anforderung des **Agenten** neu.



Installation des Dr.Web Agenten mit Installer im grafischen Modus

Um Antivirus-Software (Dr.Web Agent und Antivirus-Paket) im grafischen Modus des Netzinstallers zu installieren:

1. Auf dem Rechner, auf dem die Antivirensoftware installiert wird, starten Sie das `drwinst.exe` Programm mit dem Parameter `-interactive`. Das Programm `drwinst.exe` können Sie auf eine der folgenden Weisen finden:
   - Im Netzwerkinstallationsverzeichnis des **Agenten**. Bei Installation des **Servers** ist es das `Installer` - Unterverzeichnis (per Default versteckte geteilte Ressource) im Installationsverzeichnis des **Servers**. Im Weiteren kann es verschoben werden.
   - Auf der Installationsseite des **Dr.Web Verwaltungscenters**, die auf jedem Rechner mit dem Netzwerkzugriff auf den **Enterprise Server** verfügbar ist, unter:
     `http://`*<Serveradresse>*`:`*<Portnummer>*`/install/`
     wobei als <*Serveradresse*> die IP-Adresse oder der DNS-Name des Rechners, auf dem der **Enterprise Server** installiert ist, anzugeben ist. Als <*Portnummer*> geben Sie die Portnummer `9080` (oder `9081` für https) an.

   Es öffnet sich das Fenster vom **Dr.Web** Antivirus-Installationswizard.

2. Vor Beginn der Installation bittet der Installationswizard zu bestätigen, dass keine Antivirus-Programme auf dem Computer installiert sind. Stellen Sie sicher, dass keine andere Antivirus-Software (darunter auch andere Versionen der Antivirus-Software von **Dr.Web**) auf dem Computer benutzt wird. Danach setzen Sie ein Häkchen bei **Auf meinem Computer gibt es keine andere Antivirus-Software** und klicken Sie auf **Weiter**.
3. Im nächsten Fenster wird es angeboten, den Installationstyp zu wählen:



- **Schnellinstallation (empfehlenswert)** - die einfachste Installationsvariante. Sämtliche Parameter werden automatisch festgelegt. Gehen Sie direkt weiter zu Schritt **7**.
- **Benutzerdefinierte Installation** - Installationsvariante, bei der Sie die Komponenten der auf dem Computer zu installierenden Antivirus-Software auswählen können.
- **Administrative Installation** - die meist vollständige Installationsvariante. Dieser Installationstyp lässt sämtliche Parameter der Installation sowie der zu installierenden Antivirus-Software festlegen/ändern.

4. Bei Installationsvarianten **Benutzerdefinierte Installation** und **Administrative Installation** können Sie im nächsten Fenster die Komponenten des **Dr.Web** Antivirus-Pakets auswählen. Setzen Sie Häkchen bei den Komponenten, die Sie auf Ihrem Computer installieren möchten.

   Im Abschnitt **Pfad des Installationsordners** können Sie den Ordner festlegen, in dem die Antivirus-Software installiert wird. Standardmäßig ist es der Ordner `Dr.Web Enterprise Suite`, der sich im `Program files` Ordner auf der Systemplatte befindet. Zur Änderung des Installationspfads klicken Sie auf **Durchsuchen** und geben Sie den erforderlichen Pfad an.

   Klicken Sie auf **Weiter**.

   Bei der Installationsvariante **Benutzerdefinierte Installation** gehen Sie direkt weiter zu Schritt **7.**

5. Bei der Installationsvariante **Administrative Installation:** im nächsten Fenster legen Sie die Einstellungen des **Netzwerkinstallers** fest:



- Im Feld **Dr.Web Enterprise Server** wird die Netzwerkadresse des **Enterprise Servers** angegeben, von dem **Agent** und Antivirus-Paket installiert werden. Wenn Sie beim Starten des Installationsprogramms die Adresse des **Servers** angegeben haben, wird diese Adresse automatisch ins genannte Feld eingetragen. Falls die **Server**-Adresse Ihnen unbekannt ist, klicken Sie auf den **Suche**-Knopf. Dabei öffnet sich ein Fenster zur Suche von aktiven **Enterprise Server** des Netzwerkes. Legen Sie erforderliche Parameter (im Format *<Servername>*@ *<IP-Adresse>*/ *<Netzwerkpräfix>*: *<Port>)* fest und klicken Sie auf den **Suche**-Knopf. Aus der Liste der gefundenen **Server** wählen Sie den Server aus, von dem die Antivirus-Software installiert wird, und klicken Sie auf **OK**.
- Im Feld **Dr.Web Enterprise Server öffentlicher Schlüssel** wird der vollständige Pfad des öffentlichen Schlüssels (`drwcsd.pub`) angegeben, der sich auf Ihrem Computer befindet (wird das Installationsprogramm vom **Server** über Netzwerk gestartet, so wird der Schlüssel in die temporären Dateien des Betriebssystems kopiert und nach der Installation in den Installationsordner übertragen).
- Im Abschnitt **Komprimierung beim Herunterladen verwenden** wählen Sie gewünschte Variante zum Komprimieren des Verkehrs: **Ja** - Komprimierung verwenden, **Nein** - nicht verwenden, **Möglich** - die Verwendung der Komprimierung hängt von **Server**-Einstellungen ab.
- Das Häkchen bei **Dr.Web Agenten in die Liste der Ausnahmen von Windows Firewall hinzufügen** bestimmt das Hinzufügen von den vom **Agenten** benutzten Ports und Oberflächen in die Ausnahmenliste vom Netzwerkmonitor des Betriebssystems (außer Windows 2000 oder älter). Es ist empfehlenswert, dieses Häkchen zu setzen. Es hilft, Fehler zu vermeiden, z.B. bei automatischer Aktualisierung von Antivirus-Komponenten und Virendatenbanken.
- Setzen Sie gegebenenfalls ein Häkchen bei **Den Agenten in der Liste der installierten Programme zu registrieren**.



6. Bei der Installationsvariante **Administrative Installation:** im nächsten Fenster legen Sie die Einstellungen des **Agenten** fest:

   - Im Abschnitt **Authorisierung** werden die Parameter für Authorisierung des **Agenten** auf dem **Server** festgelegt. Bei der Auswahl der Variante **Automatisch (standard mäßig)** wird der Zugriffsmodus für Station auf dem **Server** bestimmt. Bei der Variante **Manuell** sind die Authorisierungsparameter der Station festzulegen: **Identifizierer** der Station auf dem **Server** und **Passwort** für den Zugriff darauf. Dabei bekommt die Station den Zugriff, ohne dass die manuelle Bestätigung durch den Administrator auf dem **Server** erforderlich sein wird.
   - In den Abschnitten **Komprimierung** und **Verschlüsselung** werden entsprechende Modi für den Verkehr zwischen **Server** und **Agenten** festgelegt (weitere Information s. im Punkt **Verwendung von Komprimierung und Verschlüsselung des Verkehrs** in dem Administratorhandbuch zum **Dr.Web Enterprise Security Suite Antivirus).**

   Klicken Sie auf **Weiter**.

7. Die Installation des **Dr.Web Agenten** startet. Nach der Installation des **Agenten** klicken Sie auf **Fertig,** um den Installationswizard zu beenden.
8. Nach der Bestätigung von Station auf dem **Server** (falls es durch **Server**-Einstellungen vorgesehen ist und bei Schritt **6** der **Administrativen Installation Manuell** als Authorisierungstyp nicht gewählt wurde) wird das Antivirus-Paket automatisch installiert.
9. Starten Sie Ihren Computer nach Anforderung des **Agenten** neu.

2.3.2. Deinstallation des Dr.Web Agenten



Um den **Agenten** und das Antivirus-Paket lokal zu deinstallieren, muss diese Option durch Administrator auf dem **Server** freigegeben werden.

Nach Deinstallieren der Antivirus-Software wird Ihr Computer vor Viren und anderen böswilligen Programmen nicht geschützt.

Deinstallation von Antivirus-Software der Station (des **Dr.Web Agenten** und des Antivirus-Pakets) kann auf zwei Weisen ausgeführt werden:

1. Mit Hilfe von normalen Windows-Mitteln.
2. Mit Hilfe von Installationsprogramm des Agenten.

Mit normalen Windows-Mitteln deinstallieren



Dieses Verfahren kann zum Deinstallieren nur verwendet werden, wenn ein Häkchen bei **Den Agenten in der Liste der installierten Programme zu registrieren** während Installation des **Agenten** mit Hilfe des grafischen Installationsprogramms gesetzt wurde.

Falls der **Agent** im grafischen Modus des Installationsprogramms installiert wurde, wird das Deinstallieren der Antivirus-Software mit normalen Windows-Mitteln nur in dem Fall zugänglich, wenn der –`regagent` Schlüssel bei der Installation verwendet wurde.

Zum Deinstallieren der Antivirus-Software wählen Sie:

- Für Betriebssysteme Windows 98, Windows NT4, Windows ME, Windows 2000: **Start** → **Einstellungen** → **Systemsteuerung** → **Software**.
- Für Betriebssysteme Windows XP, Windows 2003 (abhängend vom **Start**-Menü Typ):



   - Start-Menü: **Start** → **Systemsteuerung** → **Software**.
   - Klassisches Start-Menü: **Start** → **Einstellungen** → **Systemsteuerung** → **Software**.

- Für Betriebssystem Windows Vista oder neuer (abhängend vom **Start**-Menü Typ):
   - Start-Menü: **Start** → **Systemsteuerung** → **Programme**, weiter abhängend vom Typ der Systemsteuerung:
      - Klassisches Start-Menü: **Programme**.
      - Startseite: **Programme** → **Programme und Funktionen**.
   - Klassisches Start-Menü: **Start** → **Einstellungen** → **Systemsteuerung** → **Programme und Funktionen**.

In der geöffneten Liste wählen Sie die Zeile **Dr.Web Enterprise Agent** und klicken Sie auf **Löschen** (oder **Löschen/Ersetzen** für ältere Windows-Versionen). Die Antivirus-Software der Station wird deinstalliert.

Deinstallieren mit Hilfe des Installationsprogramms

Um die Software des **Dr.Web Agenten** und das Antivirus-Paket auf der Station lokal zu deinstallieren, ist es erforderlich, den `drwinst` Befehl mit dem `-uninstall` Parameter (oder mit `-uninstall -interactive` Parametern, falls es erforderlich sein wird, Kontrolle der Deinstallation sicherzustellen) im Installationsordner des **Dr.Web Agenten** (standardmäßig - `C:\Program Files\DrWeb Enterprise Suite`) auszuführen.

2.4. Benutzeroberfläche des Dr.Web Agenten starten und stoppen

Der **Dr.Web Agent** wird automatisch nach der Installation sowie jedesmal nach Windows Herunterladen gestartet.

In der Windows-Umgebung legt der gestartete **Dr.Web Agent** das Icon  im Infobereich der Taskleiste an.

Der Befehl **Beenden** im Kontextmenü des **Agenten** dient nur zum Löschen des Icons aus dem Infobereich der **Taskleiste**. Der **Agent** setzt dabei seine Funktion fort.

Nach Windows Herunterladen wird das Icon des **Agenten** automatisch nach seinem Starten im Bereich der **Taskleiste** angelegt.

Zur Anzeige des **Agenten**-Icons (falls das Icon mit Hilfe des Befehls **Beenden** gelöscht wurde) ohne Computer-Neustart kann die Benutzeroberfläche des **Agenten** mit Hilfe des Punktes **Start AgentUI** im Windows-Menü **Start** → **Programme** → **Dr.Web Enterprise Suite** gestartet werden.

Um die Benutzeroberfläche des Agenten unter einem anderen Benutzernamen (z.b. unter dem Namen eines Benutzers mit Administratorrechten) zu starten:

1. Gehen Sie zum Windows-Menü **Start** → **Programme** → **Dr. Web Enterprise Suite**.
2. Mit der rechten Maustaste klicken Sie auf den Menüpunkt **Start AgentUI** und im Kontextmenü wählen Sie die Option **Starten als.**
3. Im geöffneten Fenster geben Sie die Daten (Login und Passwort) des gewünschten Benutzerkontos an und klicken Sie auf **OK**.

   Die Benutzeroberfläche des **Agenten** wird unter dem Namen des angegeben Benutzers gestartet.



2.5. Verwaltung des Dr.Web Agenten

In der Windows-Umgebung legt der gestartete **Dr.Web Agent** das Icon im Infobereich der **Taskleiste** an.

Beim Bewegen des Mauszeigers auf das **Agenten**-Icon erscheint ein Popup-Meldefenster mit Gesamtangaben über Virenereignisse, Status von Komponenten der Antivirus-Software sowie Datum der letzten Aktualisierung (s. auch Punkt Infomeldungen).

Die zum Ändern und Anschauen zugängliche Funktionen des **Dr.Web Agenten** werden aus dem Kontextmenü des **Dr.Web Agenten**-Icons aufgerufen. Dafür klicken Sie mit der rechten Maustaste aufs Icon und wählen Sie den erforderlichen Befehl aus.



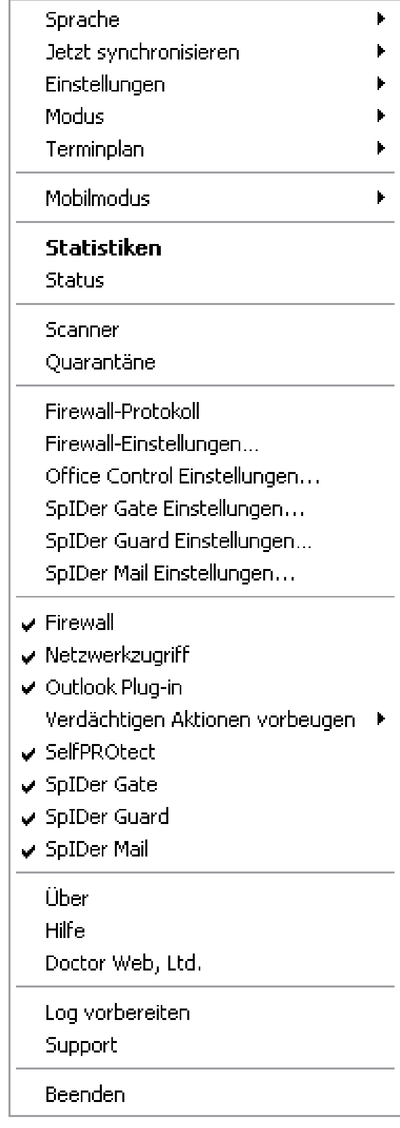


Abbildung 2-1. Kontextmenü des Dr.Web Agenten.

Das Kontextmenü enthält folgende Punkte:

- **Beenden** - das Icon des **Dr.Web Agenten** aus dem Infobereich der **Taskleiste** entfernen (s. Punkt Benutzeroberfläche des Dr.Web Agenten starten und stoppen).
- **Support** - auf Website des technischen Supportdienstes von **Doctor Web** gehen, um technische Unterstützung zu erhalten.
- **Log vorbereiten** - Archiv (im zip-Format) mit Logdateien und Systeminformation zum Versand an technischen Supportdienst erstellen.
- **Doctor Web, Ltd.** - auf Website von **Doctor Web** gehen.
- **Hilfe** - Hilfedatei des **Dr.Web Agenten** aufrufen.
- **Über** - Informationen über das Programm und aktuelle Version anschauen. Es ist auch möglich, aus diesem Meldefenster auf Website von **Doctor Web** oder auf Website des technischen Supportdienstes von **Doctor Web** zu gehen.
- **SpIDer Mail** - E-Mail-Wächter von **SpIDer Mail** aktivieren/ deaktivieren.

  SpIDer Mail prüft automatisch alle Zugriffe beliebiger E-Mail-Programme, die auf Ihrem Computer installiert sind, auf die Mailserver.

- **SpIDer Guard** - Dateiwächter von **SpIDer Guard** aktivieren/ deaktivieren.

  SpIDer Guard prüft "on the fly" alle Dateiaufrufe sowie überprüft permanent die Aktionen der gestarteten Vorgänge, die für Viren kennzeichnend sind.

- **SpIDer Gate** - HTTP-Wächter von **SpIDer Gate** aktivieren/ deaktivieren.

  SpIDer Gate hilft Ihren Computer vor Malware-Programmen, die sich beim Zusammenwirken im Netzwerk über HTTP-Protokoll übertragen werden können, zu schützen.

- **SelfPROtect** - Systemwächter **SelfPROtect** aktivieren/ deaktivieren.

  Diese Komponente schützt die Dateien und Ordner von **Dr.Web** vor unbefugtem oder zufälligem Eingreifen, z.B. vor Löschen



durch Viren. Wenn der Systemwächter aktiviert ist, haben nur **Dr. Web** Programme Zugriff auf genannte Ressourcen.

- In der ausfallenden Liste **Verdächtigen Aktionen vorbeugen** sind folgende Optionen verfügbar:
  - **HOSTS-Systemdatei schützen** setzt Verbot für Änderungen an der HOSTS-Datei durch, die durch Betriebssystem zur Vereinfachung des Internetzugangs benutzt wird, d.h. zur Umsetzung der Textnamen mancher Websites zu entsprechenden IP-Adressen. Änderung an der HOSTS-Datei kann auf Schadprogramme hindeuten.
  - **Kritische System-Objekte schützen** setzt Verbot für Änderungen an den kritischen Objekten des Betriebssystems (Registrierdatenbank usw.).
- **Outlook plug-in** - das anzuschließende **Dr.Web für Outlook** Modul aktivieren/deaktivieren.

  Dr.Web für Outlook prüft E-Mails, die mit Hilfe eines Mailprogramms empfangen/versandt werden.
- **Netzwerkzugang** - falls das Häkchen hier gesetzt wird, wird der Zugang auf das lokale Netzwerk und Internet erlaubt, anderenfalls wird es verboten.
- **Firewall** - Netzwerkmonitor von **Dr.Web Firewall** aktivieren/ deaktivieren.

  Dr.Web Firewall Netzwerkmonitor dient dem Schutz Ihres Computers vor unbefugtem Zugriff von außen sowie zur Verhinderung des Datenverlustes im Netzwerk.

Weitere Information über sonstige Menüpunkte finden Sie in nachfolgenden Kapiteln des Benutzerhandbuches. Für Übergang zum gewünschten Abschnitt klicken Sie auf entsprechenden Menüpunkt in der Abbildung 2-1.



Einstellungen, die über Kontextmenü des **Dr.Web Agenten** -Icons verfügbar sind, können sich je nach Konfiguration der Workstation unterscheiden. Der Administrator des Antivirus-Netzwerkes kann die Benutzerrechte auf Verwaltung und Einstellung der Antivirus-Produkte, die auf dem Computer des Benutzers installiert sind, beschränken.

Falls manche Punkte des Kontextmenüs unzugänglich sind, kann es durch eine der zwei Varianten verursacht werden:

1. Rechte, die diese Einstellungen ändern lassen, wurden durch den Administrator des Antivirus-Netzwerkes auf dem **Server** deaktiviert.
2. Der Benutzer hat keine Administratorrechte auf diesem Computer.

Das Kontextmenü des **Agenten**, der ohne Administratorrechte unter Windows Vista oder neuer gestartet wird, enthält einen zusätzlichen Punkt **Administrator** (s. Abb. 2-2). Dieser Menüpunkt lässt den **Dr. Web Agenten** mit Administratorrechten auf diesem Computer starten, um einen vollständigen Zugriff auf Funktionalität des **Agenten** zu gewährleisten: dabei werden alle Menüpunkte, die auf dem Antivirus-**Server** erlaubt sind, aktiv.

Das Kontextmenü des **Agenten**, der mit Administratorrechten unter Windows Vista oder neuer mit eingeschalteter UAC(Komponente von Microsoft Windows. Die UAC fordert Bestätigung der Aktionen an, die Administratorrechte bedürfen, um den Schutz des Computers vor Missbrauch zu gewährleisten. Der Administrator des Computers kann UAC im Systemsteuerung abschalten) gestartet wird, enthält den Menüpunkt **Benutzer**, der den **Agenten** ohne Administratorrechte (unter dem Namen des Benutzers) starten lässt.



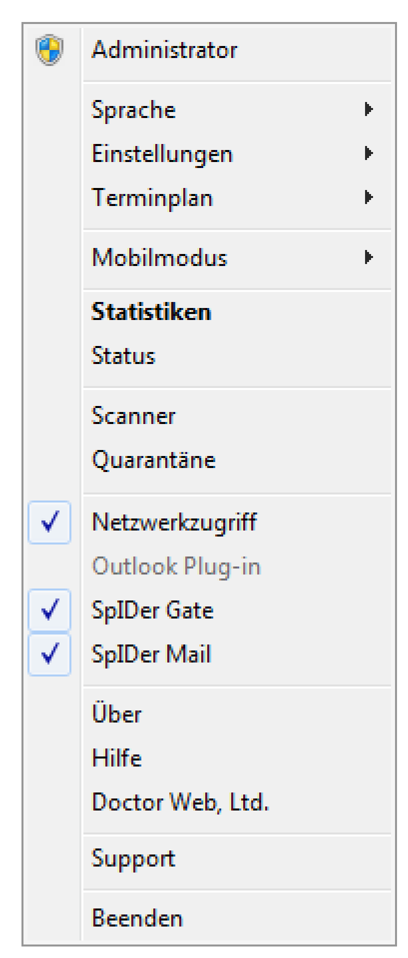


Abbildung 2-2. Kontextmenü des Dr.Web Agenten unter dem Benutzer von Windows 7



In allen Dialogfenstern des **Dr.Web Agenten** klicken Sie auf F1, um Informationen über das aktive Fenster zu erhalten. Um Kontexthilfe über ein Fensterelement zu erhalten, klicken Sie mit der rechten Maustaste darauf.

Die Darstellung des **Dr.Web Agenten**–Icons hängt davon ab, ob die Verbindung von Workstation zum **Server** aufgebaut wurde sowie von anderen Parametern. Mögliche Varianten und entsprechende Status von Komponenten sind in Tabelle 2 angeführt.

Tabelle 2. Mögliche Darstellungsvarianten des Icons und entsprechende Status von Komponenten

Icon	Beschreibung	Status
	Schwarzes Bild vor grünem Hintergrund.	**Agent** funktioniert normal und baut Verbindung zum **Server** auf.
	Rote Pfeile vor Icon-Hintergrund.	Verbindung zum **Server** fehlt.
	Ausrufezeichen im gelben Dreieck vor Icon-Hintergrund.	**Agent** fordert den Computerneustart an oder die **SelfPROtect** oder **Spider Guard** Komponente ist deaktiviert.
→	Der Icon-Hintergrund wechselt seine Farbe von Grün zum Rot.	Ein Fehler bei Aktualisierung von Paket-Komponenten ist aufgetreten.
	Der Icon-Hintergrund bleibt permanent rot.	**Agent** wurde gestoppt oder funktioniert nicht.
	Der Icon-Hintergrund ist gelb.	**Agent** funktioniert im Mobilmodus.

Kapitel 3. Funktionalität des Dr.Web Agenten

3.1. Sprache der Benutzeroberfläche einstellen



Die Änderung der Sprache in der Benutzeroberfläche von sämtlichen Antivirus-Komponenten ist nur mit dem **Dr.Web Agenten** möglich.

Um die Sprache in der Benutzeroberfläche des **Dr.Web Agenten** und der Komponenten vom **Dr.Web** Antivirus-Paket zu ändern, wählen Sie den Menüpunkt **Sprache** im Kontextmenü des **Agenten**-Icons aus. In der ausfallenden Liste geben Sie nötige Sprache der Benutzeroberfläche an.

3.2. Antivirus-Software aktualisieren

Sobald die Updates für **Dr.Web** Antivirus-Software erscheinen, werden sie automatisch geladen und installiert. Aber in kritischen Situationen können Sie die Software-Komponenten manuell aktualisieren (nachdem Sie Beratung durch den Administrator erhalten).

Die auf Ihrem Computer installierte Antivirus-Software kann über den Menüpunkt **Synchronisieren** im Kontextmenü aktualisiert werden.

- Wenn der Hintergrund des **Agenten**-Icons seine Farbe vom Grün zum Rot wechselt, heisst es, dass Sie die Komponenten, deren Update mit einem Fehler durchgelaufen ist, zwangsweise aktualisieren müssen. Dafür wählen Sie den Menüpunkt **Nur fehlerhafte Komponenten** des Befehls **Synchronisieren** im Kontextmenü aus.

- Falls es erforderlich ist, sämtliche installierte Antivirus-Komponenten zu aktualisieren (z.B wenn der **Agent** lange keine Verbindung zum **Server** hatte usw.), wählen Sie **Alle Komponenten** des Befehls **Synchronisieren** im Kontextmenü aus.

3.3. Einstellungen des Dr.Web Agenten

Zugang zu Einstellungen des **Dr.Web Agenten** ist mit Hilfe des Befehls **Einstellungen** im Kontextmenü des **Agenten** möglich.

In der ausfallenden Liste vom Menü **Einstellungen** können Sie den Typ der Meldungen über Virenereignisse auf Ihrem Computer, die Sie erhalten möchten, auswählen. Dafür setzen Sie ein Häkchen bei entsprechendem Menüpunkt (klicken Sie mit der linken Maustaste darauf):

- **Wichtige Meldungen** - nur wichtige Benachrichtigungen erhalten. Dazu gehören die Meldungen über:
    - Fehler beim Starten einer Komponente der Antivirus-Software.
    - Fehler bei der Aktualisierung der Antivirus-Software oder einer seiner Komponenten, wird gleich nach fehlerhafter Beendung des Aktualisierungsvorgangs angezeigt.
    - Notwendigkeit, den Computer nach Update neu zu starten, wird gleich nach der Aktualisierung angezeigt.
    - Notwendigkeit, auf eine Anforderung des Neustarts zur Beendung der Komponenteninstallation zu warten.
- **Nebensächliche Meldungen** - nur geringfügige Benachrichtigungen erhalten. Dazu gehören die Meldungen über:
    - Starten des Fernscannens.
    - Beendung des Fernscannens.
    - Starten der Aktualisierung von Antivirus-Software oder einer seiner Komponenten.



- Erfolgreiche Beendung der Aktualisierung von Antivirus-Software oder einer seiner Komponenten (ohne dass Neustart benötigt wird).

- **Virusmeldungen** - nur Virenmeldungen erhalten. Zu diesem Benachrichtigungstyp gehören die Meldungen beim Fund eines Virus (Viren) durch eine Komponente der Antivirus-Software.

Wenn Sie alle Meldungsgruppen erhalten möchten, setzen Sie alle drei Häkchen. Anderenfalls werden nur die Meldungen der angegebenen Gruppen angezeigt (s. auch Punkt Infomeldungen).

Um die Synchronisierung der Systemzeit mit dem **Server** zu aktivieren, setzen Sie ein Häkchen bei **Zeit synchronisieren**. In diesem Modus legt der **Agent** die Systemzeit auf Ihrem Computer gemäß der auf dem **Server** eingestellten Zeit regelmäßig fest.

Zum Anschauen oder Ändern der Verbindungsparameter zum **Server** wählen Sie den Menüpunkt **Verbindung wird hergestellt** (s. Punkt Verbindungseinstellungen zum Server) aus.

Zum Anschauen oder Ändern von Führungsparametern des Virenereignisse-Protokolls auf Ihrem Computer wählen Sie den Menüpunkt **Logniveau** (s. Punkt Detailtiefe des Protokolls) aus.



Die Menüpunkte **Zeit synchronisieren** und **Logniveau** sind im Menü **Einstellungen** nur zugänglich, wenn der Benutzer:

1. Rechte, die diese Einstellungen ändern lassen, besitzt. Die Rechte werden vom Administrator des Antivirus-Netzwerkes auf dem **Server** festgelegt.
2. Administratorrechte auf diesem Computer besitzt.

3.3.1. Verbindungseinstellungen zum Server

Zum Anschauen und Editieren der Verbindungseinstellungen zum Antivirus-**Server** gehen Sie zum Kontextmenü **Einstellungen** → **Verbindung wird hergestellt**.



Der Menüpunkt **Verbindung wird hergestellt** ist im Menü **Einstellungen** nur zugänglich, wenn der Benutzer:

1. Rechte, die diese Einstellungen ändern lassen, besitzt. Die Rechte werden vom Administrator des Antivirus-Netzwerkes auf dem **Server** festgelegt.
2. Administratorrechte auf diesem Computer besitzt.

Im Dialogfenster der Verbindungseinstellungen zum Antivirus-**Server** von **Dr.Web** (s. Abb. 3-1) können Sie die Einstellungen der Verbindung zum aktuellen **Server** ändern oder die Verbindung zu einem neuen Antivirus-**Server** einstellen.

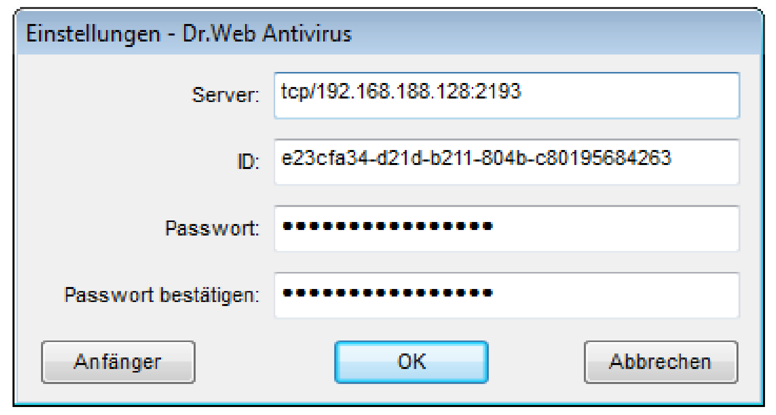


Abbildung 3-1. Verbindungseinstellungen zum Server.



In allen Dialogfenstern des **Dr.Web Agenten** klicken Sie auf F1, um Informationen über das aktive Fenster zu erhalten. Um Kontexthilfe über einen Fensterbereich zu erhalten, klicken Sie mit der rechten Maustaste darauf.



Die Verbindungseinstellungen zum Antivirus-**Server** können nur in Abstimmung mit dem Administrator des Antivirus-Netzwerkes geändert werden, ansonsten wird Ihr Computer vom Antivirus-Netzwerk abgeschaltet.



Gegebenenfalls können Sie Parameter ändern:

- **Server** - geben Sie den Namen des Antivirus-**Servers** oder seine IP-Adresse ein.
- **ID** - geben Sie den Identifizierer des **Dr.Web Agenten** an, der Ihrem Computer für seine Registrierung auf dem **Server** zugeordnet wird.
- **Passwort** - geben Sie das Passwort des **Dr.Web Agenten** für Verbindung zum Antivirus-**Server** ein. Im Feld **Passwort bestätigen** geben Sie dasselbe Passwort wiederholt ein.

Um das Fenster zu verlassen und Änderungen zu speichern, klicken Sie auf **OK**.

Um das Fenster zu verlassen, ohne dabei die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Um alle Verbindungseinstellungen zum **Server** zurückzusetzen, klicken Sie auf den **Anfänger**-Knopf. In diesem Fall verliert der **Agent** seine Verbindung zum Antivirus-**Server** und der maximal zuverlässige Schutz Ihres Computers durch das Antivirus-Paket wird dadurch unmöglich. Um später die Verbindung zum **Server** neu einzustellen, müssen Sie in diesem Dialogfenster neue Registrierungsdaten auf dem **Server** angeben. Nachdem die Registrierung durch den Administrator des Antivirus-Netzwerkes bestätigt wird, wird Ihr Computer wieder zum Antivirus-**Server** angeschlossen.

3.3.2. Detailtiefe des Protokolls

Um die Detailtiefe des Ereignis-Protokolls auf Ihrem Computer zu ändern, gehen Sie zum Kontextmenü **Einstellungen** → **Logniveau**.



Der Menüpunkt **Logniveau** ist im Menü **Einstellungen** nur zugänglich, wenn der Benutzer:

1. Rechte, die diese Einstellungen ändern lassen, besitzt. Die Rechte werden vom Administrator des Antivirus-Netzwerkes auf dem **Server** festgelegt.
2. Administratorrechte auf diesem Computer besitzt.

In der ausfallenden Liste wählen Sie den erforderlichen Wert aus (**Fehlerbeseitigung 3** – maximal detaillierte Protokollführung, **Kritische Fehler** – minimal detaillierte Protokollführung, bei der nur Fehlermeldungen gespeichert werden):

- **Fehlerbeseitigung 3 ... Fehlerbeseitigung -** Debugging-Meldungen mit unterschiedlicher Detailtiefe,
- **Ablaufverfolgung 3 ... Ablaufverfolgung -** Überwachung der geschehenden Ereignisse mit unterschiedlicher Detailtiefe,
- **Informationen** - Infomeldungen,
- **Bemerkung** - wichtige Infomeldungen,
- **Warnung** - Warnungen vor möglichen Fehlern,
- **Fehler** - Meldungen über Funktionsfehler,
- **Kritische Fehler** - Meldungen über kritische Funktionsfehler.

3.4. Modus des Zusammenwirkens zwischen dem Agenten und dem Server

Die Parameteränderung des Zusammenwirkens zwischen dem **Dr.Web Agenten** und dem **Server** erfolgt mit dem Befehl **Modus** im Kontextmenü des **Agenten**.



Der Menüpunkt **Modus** ist im Kontextmenü des **Agenten** nur zugänglich, wenn der Besitzer:

1. Rechte, die diese Einstellungen ändern lassen, besitzt. Die Rechte werden vom Administrator des Antivirus-Netzwerkes auf dem **Server** festgelegt.
2. Administratorrechte auf diesem Computer besitzt.

In der ausfallenden Liste **Modus** sind folgende Menüpunkte verfügbar:

- **Mit Dr.Web Enterprise Server verbinden** - zum Versand der Statistiken an Administrator sowie zum Erhalten der **Dr.Web** Anleitungen und Updates vom **Server**.
- **Aufgaben akzeptieren** - zum regelmäßigen Erhalten der Aufgaben für Virenprüfung Ihres Computers vom Administrator.



- **Updates akzeptieren** - zum Erhalten der regelmäßigen Updates von Antivirus-Komponenten und Virendatenbanken.
- **Ereignisse sammeln** - zum Speichern und Deaktivieren des Statistik-Versandes über Virenereignisse auf Ihrem Computer.

  Bei aktivierter Option setzt der **Agent** sein Zusammenwirken mit dem **Server** fort, dabei aber werden folgende Informationen dem **Server** nicht zugesandt:

  - regelmäßige Statistik,
  - vireninformation,
  - änderung von Konfiguration des **Agenten** und der Antivirus-Komponenten,
  - information über Starten und Stoppen der Antivirus-Komponenten.

  Diese Informationen sind nicht kritisch und haben keine Einwirkung auf Funktion des **Agenten**.

  Diese Informationen werden dabei gespeichert und bei nächster Verbindung zum **Server** versandt, nachdem die Option **Ereignisse speichern** deaktiviert wird.



Diese Option kann bei niedriger Kanalleistung nützlich sein.

3.5. Terminplan einstellen

Je nach Einstellungen auf dem **Server** können Sie den Terminplan des Antivirus-**Scanners** anschauen und editieren:

- lokalen Terminplan für Prüfungen festsetzen und ändern;
- zentralisierten Terminplan für Prüfungen anschauen.

Dafür müssen Sie den entsprechenden Menüpunkt in der ausfallenden Liste des Befehls **Terminplan** im Kontextmenü des **Agenten** auswählen.



3.5.1. Lokaler Terminplan. Liste der lokalen Aufgaben

Je nach Einstellungen auf dem **Server** können Sie Ihren eigenen Terminplan aufstellen und dazu unterschiedliche Typen von Aufgaben für Prüfung von Ihrem Computer hinzufügen.



Der Menüpunkt **Lokalterminplan** ist im Menü **Terminplan** nur zugänglich, wenn der Besitzer:

1. Rechte, die diese Einstellungen ändern lassen, besitzt. Die Rechte werden vom Administrator des Antivirus-Netzwerkes auf dem **Server** festgelegt.
2. Administratorrechte auf diesem Computer besitzt.

Wird der Punkt **Lokalterminplan** im Menü **Terminplan** des Kontextmenüs ausgewählt, öffnet sich das Fenster mit ihrem eigenen Terminplan.

Wenn Sie eine Aufgabe zum Scannen Ihres Computers geben möchten, klicken Sie auf **Hinzufügen**. Im geöffneten Menü wählen Sie den Typ der Aufgabe aus:

- Stündlich
- Täglich
- Wöchentlich
- Monatlich
- Jede N Minuten
- Beim Start

Falls eine der gegebenen Aufgaben in der Folgezeit editiert werden muss, wählen Sie diese Aufgabe in der Liste aus und klicken Sie auf **Bearbeiten**.

Um die Aufgabe zu löschen, wählen Sie diese in der Liste aus und klicken Sie auf **Löschen**.

Um den Scanvorgang sofort zu starten, wählen Sie den Befehl **Scanner** im Kontextmenü des Dr.Web Agenten-Icons oder im Windows Menü **Start**, Menüpunkt **Programme** aus.



In allen Dialogfenstern des **Dr.Web Agenten** klicken Sie auf F1, um Informationen über das aktive Fenster zu erhalten. Um Kontexthilfe über einen Fensterbereich zu erhalten, klicken Sie mit der rechten Maustaste darauf.

3.5.1.1. Stündliche Aufgabe

Dieser Typ der Aufgabe wird zur angegebenen Minute stündlich ausgeführt.

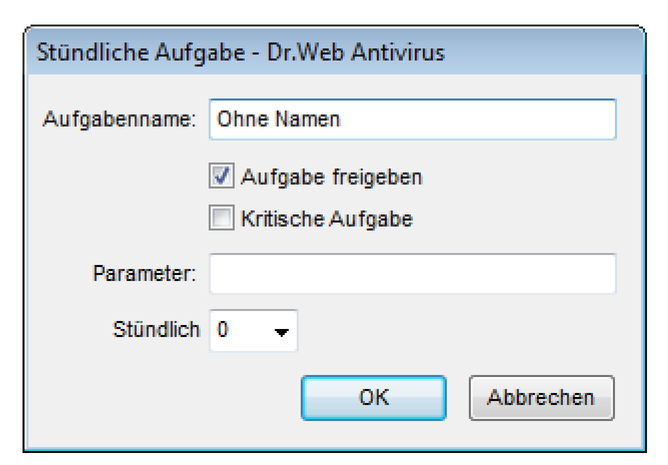


Abbildung 3-2. Dialogfenster der stündlichen Aufgabe



In allen Dialogfenstern des **Dr.Web Agenten** klicken Sie auf F1, um Informationen über das aktive Fenster zu erhalten. Um Kontexthilfe über einen Fensterbereich zu erhalten, klicken Sie mit der rechten Maustaste darauf.

Im Dialogfenster der stündlichen Aufgabe (s. Abb. 3-2) können Sie folgende Parameter festsetzen:

- **Aufgabenname** - geben Sie den Namen der Aufgabe ein.
- Setzen Sie ein Häkchen bei **Aufgabe freigeben**, um die Ausführung der Aufgabe zu erlauben.

  Um die Ausführung der Aufgabe zu verbieten, entfernen Sie das Häkchen. Dabei bleibt die Aufgabe in der Liste, wird aber nicht ausgeführt.

- Das bei **Kritische Aufgabe** gesetzte Häkchen fordert die Ausführung der Aufgabe beim nächsten Start des **Dr.Web Agenten** an, falls die Ausführung dieser Aufgabe übersprungen wird (**Dr.Web Agent** ist während der Ausführung der Aufgabe deaktiviert). Wird die Aufgabe innerhalb von einer bestimmten Zeitperiode mehrmals übersprungen, so wird sie beim Starten des **Dr.Web Agenten** einmal ausgeführt.
- **Parameter** - geben Sie gegebenenfalls zusätzliche Parameter zum Starten der Aufgabe an. Dabei werden die Parameter der Befehlszeile verwendet, die im Anhang Befehlszeilenschlüssel für Scanner angegeben sind.
- **Stündlich** - geben Sie an, zu welcher Minute stündlich die Aufgabe auszuführen ist.

Um das Fenster zu verlassen und die Parameter der Aufgabe zu speichern, klicken Sie auf **OK**.

Um das Fenster zu verlassen, ohne dabei die Änderungen/neue Aufgabe zu speichern, klicken Sie auf **Abbrechen**.



3.5.1.2. Tägliche Aufgabe

Dieser Typ der Aufgabe wird zur angegebenen Zeit jeden Tag ausgeführt.

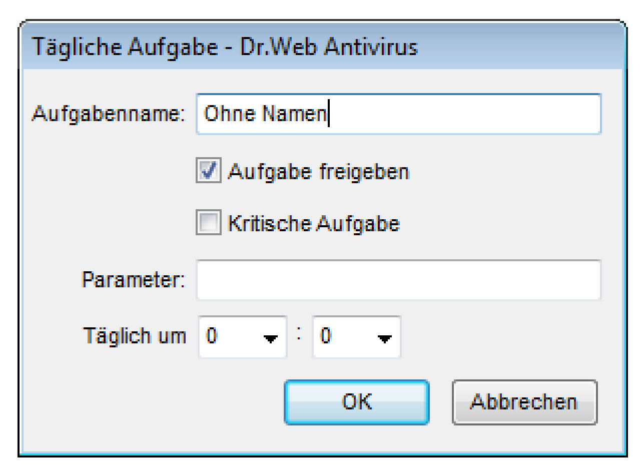


Abbildung 3-3. Dialogfenster der täglichen Aufgabe



In allen Dialogfenstern des **Dr.Web Agenten** klicken Sie auf F1, um Informationen über das aktive Fenster zu erhalten. Um Kontexthilfe über einen Fensterbereich zu erhalten, klicken Sie mit der rechten Maustaste darauf.

Im Dialogfenster der täglichen Aufgabe (s. Abb. 3-3) können Sie folgende Parameter festsetzen:

- **Aufgabenname** - geben Sie den Namen der Aufgabe ein.
- Setzen Sie ein Häkchen bei **Aufgabe freigeben**, um die Ausführung der Aufgabe zu erlauben.

  Um die Ausführung der Aufgabe zu verbieten, entfernen Sie das Häkchen. Dabei bleibt die Aufgabe in der Liste, wird aber nicht ausgeführt.

- Das bei **Kritische Aufgabe** gesetzte Häkchen fordert die Ausführung der Aufgabe beim nächsten Start des **Dr.Web**

Agenten an, falls die Ausführung dieser Aufgabe übersprungen wird (**Dr.Web Agent** ist während der Ausführung der Aufgabe deaktiviert). Wird die Aufgabe innerhalb von einer bestimmten Zeitperiode mehrmals übersprungen, so wird sie beim Starten des **Dr.Web Agenten** einmal ausgeführt.

- **Parameter** - geben Sie gegebenenfalls zusätzliche Parameter zum Starten der Aufgabe an. Dabei werden die Parameter der Befehlszeile verwendet, die im Anhang Befehlszeilenschlüssel für Scanner angegeben sind.
- **Täglich um** - geben Sie an, zu welcher Stunde und Minute täglich die Aufgabe auszuführen ist.

Um das Fenster zu verlassen und die Parameter der Aufgabe zu speichern, klicken Sie auf **OK**.

Um das Fenster zu verlassen, ohne dabei die Änderungen/neue Aufgabe zu speichern, klicken Sie auf **Abbrechen**.

3.5.1.3. Wöchentliche Aufgabe

Dieser Typ der Aufgabe wird zur angegebenen Zeit am angegebenen Wochentag jede Woche ausgeführt.

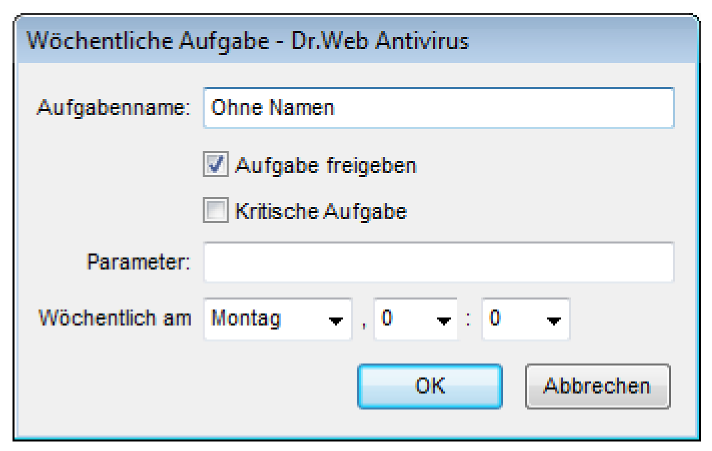


Abbildung 3-4. Dialogfenster der wöchentlichen Aufgabe





In allen Dialogfenstern des **Dr.Web Agenten** klicken Sie auf F1, um Informationen über das aktive Fenster zu erhalten. Um Kontexthilfe über einen Fensterbereich zu erhalten, klicken Sie mit der rechten Maustaste darauf.

Im Dialogfenster der wöchentlichen Aufgabe (s. Abb. 3-4) können Sie folgende Parameter festsetzen:

- **Aufgabenname** - geben Sie den Namen der Aufgabe ein.
- Setzen Sie ein Häkchen bei **Aufgabe freigeben**, um die Ausführung der Aufgabe zu erlauben.

  Um die Ausführung der Aufgabe zu verbieten, entfernen Sie das Häkchen. Dabei bleibt die Aufgabe in der Liste, wird aber nicht ausgeführt.

- Das bei **Kritische Aufgabe** gesetzte Häkchen fordert die Ausführung der Aufgabe beim nächsten Start des **Dr.Web Agenten** an, falls die Ausführung dieser Aufgabe übersprungen wird (**Dr.Web Agent** ist während der Ausführung der Aufgabe deaktiviert). Wird die Aufgabe innerhalb von einer bestimmten Zeitperiode mehrmals übersprungen, so wird sie beim Starten des **Dr.Web Agenten** einmal ausgeführt.
- **Parameter** - geben Sie gegebenenfalls zusätzliche Parameter zum Starten der Aufgabe an. Dabei werden die Parameter der Befehlszeile verwendet, die im Anhang Befehlszeilenschlüssel für Scanner angegeben sind.
- **Wöchentlich am** - geben Sie an, am welchen Wochentag, zu welcher Stunde und Minute wöchentlich die Aufgabe auszuführen ist.

Um das Fenster zu verlassen und die Parameter der Aufgabe zu speichern, klicken Sie auf **OK**.

Um das Fenster zu verlassen, ohne dabei die Änderungen/neue Aufgabe zu speichern, klicken Sie auf **Abbrechen**.



3.5.1.4. Monatliche Aufgabe

Dieser Typ der Aufgabe wird zur angegebenen Zeit am angegebenen Monatstag jeden Monat ausgeführt.

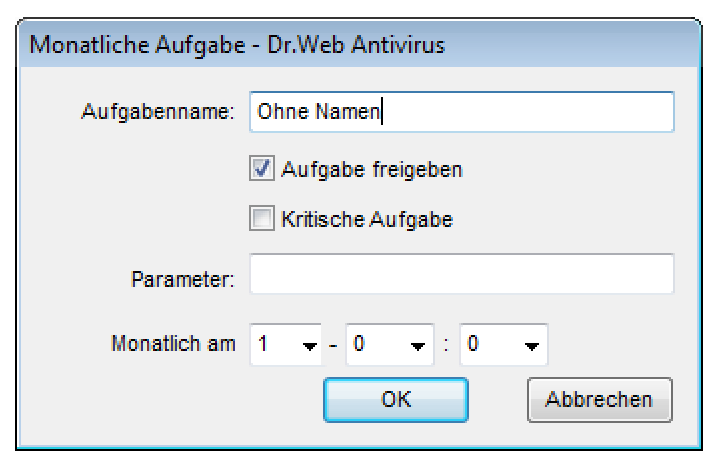


Abbildung 3-5. Dialogfenster der monatlichen Aufgabe



In allen Dialogfenstern des **Dr.Web Agenten** klicken Sie auf F1, um Informationen über das aktive Fenster zu erhalten. Um Kontexthilfe über einen Fensterbereich zu erhalten, klicken Sie mit der rechten Maustaste darauf.

Im Dialogfenster der monatlichen Aufgabe (s. Abb. 3-5) können Sie folgende Parameter festsetzen:

- **Aufgabenname** - geben Sie den Namen der Aufgabe ein.
- Setzen Sie ein Häkchen bei **Aufgabe freigeben**, um die Ausführung der Aufgabe zu erlauben.

  Um die Ausführung der Aufgabe zu verbieten, entfernen Sie das Häkchen. Dabei bleibt die Aufgabe in der Liste, wird aber nicht ausgeführt.
- Das bei **Kritische Aufgabe** gesetzte Häkchen fordert die Ausführung der Aufgabe beim nächsten Start des **Dr.Web**

Agenten an, falls die Ausführung dieser Aufgabe übersprungen wird (**Dr.Web Agent** ist während der Ausführung der Aufgabe deaktiviert). Wird die Aufgabe innerhalb von einer bestimmten Zeitperiode mehrmals übersprungen, so wird sie beim Starten des **Dr.Web Agenten** einmal ausgeführt.

- **Parameter** - geben Sie gegebenenfalls zusätzliche Parameter zum Starten der Aufgabe an. Dabei werden die Parameter der Befehlszeile verwendet, die im Anhang Befehlszeilenschlüssel für Scanner angegeben sind.
- **Monatlich am** - geben Sie an, am welchen Monatstag, zu welcher Stunde und Minute monatlich die Aufgabe auszuführen ist.

Um das Fenster zu verlassen und die Parameter der Aufgabe zu speichern, klicken Sie auf **OK**.

Um das Fenster zu verlassen, ohne dabei die Änderungen/neue Aufgabe zu speichern, klicken Sie auf **Abbrechen**.

3.5.1.5. Aufgabe, die jede X Minuten auszuführen ist

Dieser Typ der Aufgabe wird mit bestimmten Zeitabständen, die in Minuten festgesetzt sind, ausgeführt.



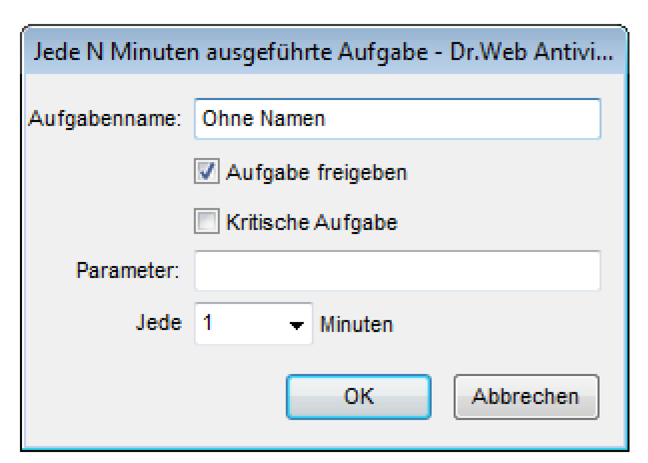


Abbildung 3-6. Dialogfenster der Aufgabe



In allen Dialogfenstern des **Dr.Web Agenten** klicken Sie auf F1, um Informationen über das aktive Fenster zu erhalten. Um Kontexthilfe über einen Fensterbereich zu erhalten, klicken Sie mit der rechten Maustaste darauf.

Im Dialogfenster der Aufgabe (s. Abb. 3-6) können Sie folgende Parameter festsetzen:

- **Aufgabenname** - geben Sie den Namen der Aufgabe ein.
- Setzen Sie ein Häkchen bei **Aufgabe freigeben**, um die Ausführung der Aufgabe zu erlauben.

  Um die Ausführung der Aufgabe zu verbieten, entfernen Sie das Häkchen. Dabei bleibt die Aufgabe in der Liste, wird aber nicht ausgeführt.

- Das bei **Kritische Aufgabe** gesetzte Häkchen fordert die Ausführung der Aufgabe beim nächsten Start des **Dr.Web Agenten** an, falls die Ausführung dieser Aufgabe übersprungen wird (**Dr.Web Agent** ist während der Ausführung der Aufgabe deaktiviert). Wird die Aufgabe innerhalb von einer bestimmten Zeitperiode mehrmals übersprungen, so wird sie beim Starten des **Dr.Web Agenten** einmal ausgeführt.

- **Parameter** - geben Sie gegebenenfalls zusätzliche Parameter zum Starten der Aufgabe an. Dabei werden die Parameter der Befehlszeile verwendet, die im Anhang Befehlszeilenschlüssel für Scanner angegeben sind.
- **Jede <...> Minuten** - geben Sie einen Zeitabstand in Minuten an, mit dem die Aufgabe ausgeführt wird.

Um das Fenster zu verlassen und die Parameter der Aufgabe zu speichern, klicken Sie auf **OK**.

Um das Fenster zu verlassen, ohne dabei die Änderungen/neue Aufgabe zu speichern, klicken Sie auf **Abbrechen**.

3.5.1.6. Aufgabe, die beim Starten auszuführen ist

Dieser Typ der Aufgabe wird beim Einschalten des Computers (Starten des Betriebssystems) ausgeführt.

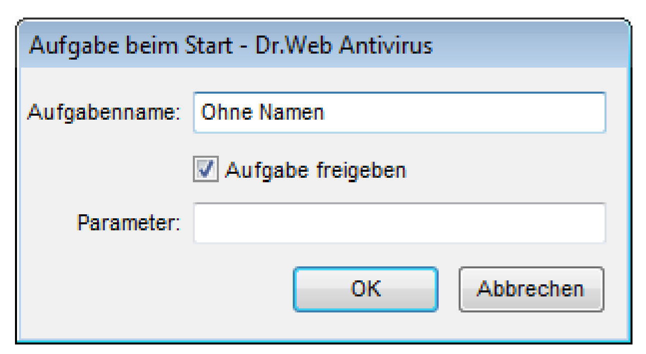


Abbildung 3-7. Dialogfenster der Aufgabe



In allen Dialogfenstern des **Dr.Web Agenten** klicken Sie auf F1, um Informationen über das aktive Fenster zu erhalten. Um Kontexthilfe über einen Fensterbereich zu erhalten, klicken Sie mit der rechten Maustaste darauf.



Im Dialogfenster der Aufgabe (s. Abb. 3-7) können Sie folgende Parameter festsetzen:

- **Aufgabenname** - geben Sie den Namen der Aufgabe ein.
- Setzen Sie ein Häkchen bei **Aufgabe freigeben**, um die Ausführung der Aufgabe zu erlauben.

  Um die Ausführung der Aufgabe zu verbieten, entfernen Sie das Häkchen. Dabei bleibt die Aufgabe in der Liste, wird aber nicht ausgeführt.

- **Parameter** - geben Sie gegebenenfalls zusätzliche Parameter zum Starten der Aufgabe an. Dabei werden die Parameter der Befehlszeile verwendet, die im Anhang Befehlszeilenschlüssel für Scanner angegeben sind.

Um das Fenster zu verlassen und die Parameter der Aufgabe zu speichern, klicken Sie auf **OK**.

Um das Fenster zu verlassen, ohne dabei die Änderungen/neue Aufgabe zu speichern, klicken Sie auf **Abbrechen**.

3.5.2. Zentralisierter Terminplan

Im Fenster des zentralisierten Terminplans für Prüfungen können Sie die auf dem Antivirus-**Server** gegebenen Aufgaben zum Scannen der Computer im Antivirus-Netzwerk anschauen.



In allen Dialogfenstern des **Dr.Web Agenten** klicken Sie auf F1, um Informationen über das aktive Fenster zu erhalten. Um Kontexthilfe über einen Fensterbereich zu erhalten, klicken Sie mit der rechten Maustaste darauf.

3.6. Einstellungen des Mobilmodus

Wenn Ihr Computer (oder Notebook) lange keine Verbindung zum Antivirus-**Server** hat, ist es empfehlenswert, den Mobilmodus des **Dr.**



Web Agenten zum rechtzeitigen Erhalten der Updates von den **Dr. Web GAS-Servern** zu installieren.

Dafür wählen Sie den Menüpunkt **Mobilmodus** → **Freigegeben** im Kontextmenü des **Agenten**-Icons aus. Die Farbe des **Agenten**-Icons wechselt zum gelb.

Im Mobilmodus versucht der **Agent** eine Verbindung zum **Server** aufzubauen, wobei er drei Versuche ausführt. Beim Fehlversuch wird das HTTP-Update von den **Dr.Web GAS-Servern** ausgeführt. Die Versuche, den **Server** zu finden, erfolgen mit einem Zeitabstand von ca. einer Minute.



Der Punkt **Mobilmodus** wird im Kontextmenü nur zugänglich, wenn der Mobilmodus von **DR.Web GAS** Nutzung in den Station-Rechten auf dem **Server** freigegeben ist.

Um die Einstellungen des Mobilmodus festzusetzen, wählen Sie **Mobilmodus** → **Einstellungen** aus. Dabei öffnet sich ein Fenster zur Einstellung von Übertragbarkeit des **Agenten**.



Abbildung 3-8. Dialogfenster zur Einstellung des Mobilmodus



In allen Dialogfenstern des **Dr.Web Agenten** klicken Sie auf F1, um Informationen über das aktive Fenster zu erhalten. Um Kontexthilfe über ein Fensterelement zu erhalten, klicken Sie mit der rechten Maustaste darauf.

Im Bereich **Aktualisierungsperiode** geben Sie an, wie oft die Prüfung von Updates im **GAS** ausgeführt werden soll:

- **20 Minuten** - Aktualisierungen jede 20 Minuten prüfen.
- **40 Minuten** - Aktualisierungen jede 40 Minuten prüfen.
- **1 Stunde** - Aktualisierungen jede Stunde prüfen.
- **2 Stunden** - Aktualisierungen jede 2 Stunden prüfen.
- **4 Stunden** - Aktualisierungen jede 4 Stunden prüfen.
- **8 Stunden** - Aktualisierungen jede 8 Stunden prüfen.
- **12 Stunden** - Aktualisierungen jede 12 Stunden prüfen.
- **1 Tag** - Aktualisierungen einmal pro Tag prüfen.

Setzen Sie ein Häkchen bei **Nur bei der Internetverbindung**, falls es erforderlich sein wird, dass die Prüfung von Aktualisierungen nur bei einer aufgebauten Internetverbindung ausgeführt wird.

Wenn ein Proxy-Server benutzt wird, setzen Sie ein Häkchen bei **Proxy-Server verwenden**. In diesem Fall werden folgende Felder aktiv:

- **Adresse** - zur Angabe der Adresse und des Ports vom Proxy-Server.
- **Anmelden** - zur Angabe der Authorisierungsparameter auf dem Proxy-Server: Login und Passwort.

Um den Aktualisierungsvorgang im Mobilmodus sofort zu starten, wählen Sie den Menüpunkt **Mobilmodus** → **Aktualisierung starten** im Kontextmenü des **Agenten** aus.



Während der **Agent** im Mobilmodus funktioniert, wird die Verbindung des **Agenten** zum **Enterprise Server** unterbrochen. Alle Änderungen, die für solche Station auf dem Server festgelegt werden, treten in Kraft, sobald der Mobilmodus des **Agenten** deaktiviert und die Verbindung des **Agenten** zum Server wiederhergestellt wird. Im Mobilmodus werden nur die Virendatenbanken aktualisiert.

Um den Mobilmodus zu deaktivieren, wählen Sie den Menüpunkt **Mobilmodus** im Kontextmenü des **Agenten** aus und entfernen Sie



das Häkchen bei **Freigeben**. Die Farbe des **Agenten**-Icons wechselt vom Gelb zum Grün. Die Verbindung des **Agenten** zum **Server** wird wieder aufgebaut.

3.7. Statistik ansehen

Zum Ansehen der Statistik für Workstation wählen Sie den Menüpunkt **Statistik** im Kontextmenü des **Agenten** aus oder klicken Sie mit der linken Maustaste zweimal auf das **Agenten**-Icon. Dabei öffnet sich ein Fenster mit der Tabelle, in der die ganze Statistik über die Funktion der Antivirus-Software enthalten ist.

In der ersten Spalte der Tabelle sind die **Dr.Web** Komponenten aufgelistet, die auf Ihrem Computer innerhalb von der laufenden Sitzung wenigstens einmal gestartet wurden. Falls dabei die Komponente kein Scannen ausgeführt hat (keine gescannten Objekte), wird diese Komponente in der Statistikliste nicht angezeigt.

In übrigen Spalten ist die Anzahl der Objekte angezeigt, die innerhalb von der laufenden Sitzung gescannt wurden.

Die Objekte werden in folgende Kategorien aufgeteilt:

- Infizierte Objekte, die vom Antivirus gefunden wurden,
- Virenmodifikationen,
- Verdächtige,
- Virenaktivitäten.

Dann wird die Anzahl der Objekte angegeben, bei denen folgende Aktionen ausgeführt wurden:

- desinfiziert,
- gelöscht,
- umbenannt,
- verschoben,
- blockiert.

Weiter finden Sie Informationen über die Anzahl der Fehler und Scan-Geschwindigkeit.



Mehr zu diesen Statistikkategorien finden Sie im Abschnitt **Statistik Tab** in der Anleitung **Dr.Web Antivirus für Windows**, die allen **Dr. Web** Antivirus-Programmen beigelegt wird.



In allen Dialogfenstern des **Dr.Web Agenten** klicken Sie auf F1, um Informationen über das aktive Fenster zu erhalten. Um Kontexthilfe über ein Fensterelement zu erhalten, klicken Sie mit der rechten Maustaste darauf.

3.8. Status der Antivirus-Software ansehen

Um den Status der auf der Workstation installierten Antivirus-Software anzuschauen, wählen Sie den Menüpunkt **Status** im Kontextmenü des **Agenten** aus.

Im oberen Bereich des geöffneten Fensters ist die Gesamtinformation enthalten:

- Gesamtanzahl der Einträge in der Virendatenbank,
- Datum der letzten Aktualisierung,
- Version des auf der Workstation funktionierenden **Agenten**,
- Scanner-Aktivität (ob der Scanner zu diesem Zeitpunkt auf der Station läuft).

Das Status-Fenster enthält auch folgende Tabs:

- **Virendatenbanken.** Enthält ausführliche Information über sämtliche installierte Virendatenbanken:
  - Name der Datei, die bestimmte Virendatenbank enthält,
  - Version der Virendatenbank,
  - Anzahl der Einträge in der Virendatenbank,
  - Erstelldatum der Virendatenbank.
- **Komponenten.** Enthält ausführliche Information über sämtliche auf der Workstation installierten **Dr.Web** Antivirus-Komponenten:



- Name der Komponente,
- Status der Komponente: gestartet (läuft) oder nicht gestartet (läuft nicht).

- **Module.** Enthält ausführliche Information über sämtliche **Dr. Web** Antivirus-Module:
  - Datei, die einzelnes Modul des Produktes definiert,
  - vollständige Modulversion,
  - Modulbeschreibung – sein Funktionsname.

Im unteren Bereich des Fensters werden folgende Informationen angezeigt:

- Statuszeile der Antivirus-Software. Enthält wichtige Meldungen (s. Punkt Einstellungen des Dr.Web Agenten). Bei normaler Funktion des **Agenten** wird die Meldung **Aktion nicht erforderlich** angezeigt;
- ID (einzigartige Identitätsnummer) des **Agenten**.



In allen Dialogfenstern des **Dr.Web Agenten** klicken Sie auf F1, um Informationen über das aktive Fenster zu erhalten. Um Kontexthilfe über ein Fensterelement zu erhalten, klicken Sie mit der rechten Maustaste darauf.

3.9. Infomeldungen

Der Benachrichtigung des Benutzers dienen die Popup-Fenster, die direkt beim Icon des **Dr.Web Agenten** untergebracht werden.

Die Meldungen in den Popup-Fenstern können unterschiedliche Informationen enthalten:

- Benachrichtigungen - ausführliche Information über ausführbare oder erforderliche Aktionen für Antivirus-Software oder Ihren Computer.
- Sammelmeldung des **Dr.Web Agenten** - Gesamtdaten über Funktion und Status der Antivirus-Software.



- Meldungen vom Administrator.

Benachrichtigungen

Mit Hilfe von Infomeldungen werden die Benachrichtigungen über Virenereignisse und Aktionen der Antivirus-Software auf Ihrem Computer angezeigt (mehr dazu s. Punkt Einstellungen des Dr. WebAgenten).

Außer informativen Funktionen können die Popup-Meldungen auch Steuerfunktionen haben. Das Fenster über erforderlichen Neustart des Computers nach Aktualisierung der Antivirus-Komponenten (s. Abb.3-9) ist z.B. im Dialogformat ausgeführt und ist mit Knöpfen versehen, die den Computer neu starten oder die Anforderung zum Neustart des Computers um die angegebene Zeit verschieben lassen. Um den Neustart zu verschieben, wählen Sie den nötigen Zeitabstand in der ausfallenden Liste aus und klicken Sie auf **Später**.

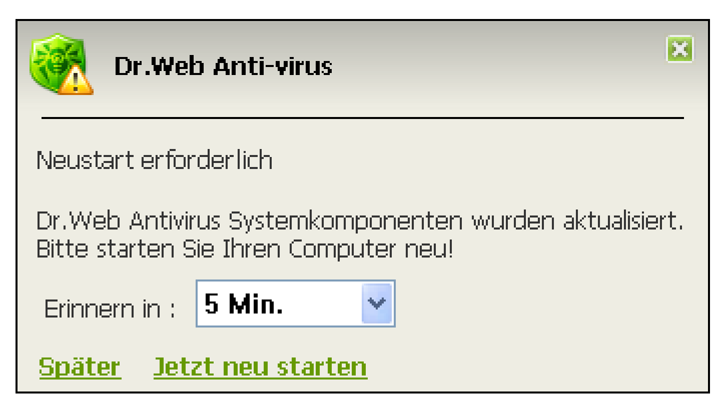


Abbildung 3-9. Benachrichtigung vom Dr.Web Agenten

Sammelmeldung des Dr.Web Agenten

Beim Bewegen des Mauszeigers über das Icon des **Dr.Web Agenten** wird ein Popup-Meldefenster mit folgenden Gesamtdaten angezeigt:

- Statistik der Virenereignisse (s. auch Punkt Statistik ansehen).



- Status von Komponenten der Antivirus-Software.
- Datum der letzten Aktualisierung.

Dr.Web Anti-virus

Geprüft:	4323 (1229 MB)
Infiziert:	0
Modifikationen:	0
Verdächtig:	0
Aktivität:	0
Desinfiziert:	0
Gelöscht:	0
Umbenannt:	0
In Quarantäne:	0
Blockiert:	0
Kein Zugriff:	5
SpIDer Guard:	läuft
SpIDer Mail:	läuft
SpIDer Gate:	läuft
Firewall:	läuft
SelfPROtect:	läuft
Agent:	läuft
Virensignaturen insgesamt:	2 090 957
Zuletzt aktualisiert am:	17:08 Montag, 16. Mai 2011

Abbildung 3-10. Meldefenster des Dr.Web Agenten

Meldungen vom Administrator

Der Benutzer kann vom Systemadministrator des Antivirus-Netzwerkes Infomeldungen mit beliebigem Inhalt erhalten. Diese Infomeldungen enthalten:

- Text der Meldung.
- Hyperlinks auf Internet-Ressourcen.
- Logo des Unternehmens (oder beliebige grafische Darstellung).
- im Fenster-Header wird auch das genaue Empfangsdatum der Meldung angegeben.

Diese Meldungen werden in Form von Popup-Fenstern angezeigt (s. Abb. 3-11).

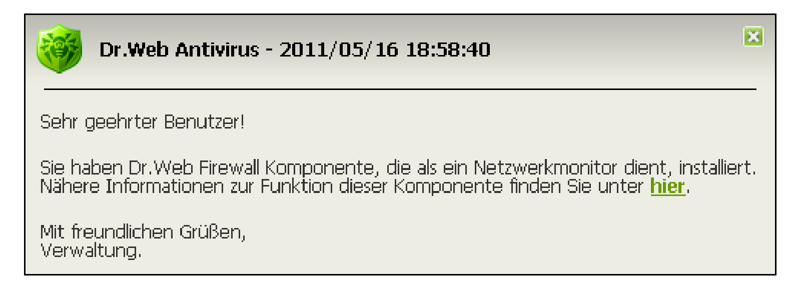


Abbildung 3-11. Meldefenster vom Administrator



Bei Inaktivität werden die Popup-Fenstern mit Benachrichtigungen und Sammelmeldungen des **Dr.Web Agenten** nach Ablauf einer bestimmten Zeit versteckt. Im Gegensatz dazu werden die Fenster mit den Meldungen vom Administrator angezeigt, bis sie vom Benutzer selbst geschlossen werden.



Kapitel 4. Antivirus-Scanner

Mit Hilfe des Befehls **Scanner** aus dem Kontextmenü des **Agenten** können Sie den **Dr.Web Antivirus-Scanner** zur regelmäßigen Prüfung Ihres Computers auf Viren und Schadprogramme starten. Dabei öffnet sich das Hauptfenster des Scanners (mehr dazu s. Anleitung **Dr.Web Antivirus für Windows**, Abschnitt **Hauptfenster des Scanners**), in dem Sie nach Vorprüfung des Computers das Antivirus-Scannen in einem der zugänglichen Modi starten können.

Je nach Einstellungen auf dem **Server** können Sie auch die Parameter der Virenprüfung optimieren: Objekte für Prüfung, Type der Aktionen bei gefundenen Objekten und sonstiges in Scanner-Einstellungen auswählen (mehr dazu s. Anleitung **Dr.Web Antivirus für Windows,** Abschnitt **Dr.Web Scanner für Windows**).



Für den Übergang zur Hilfedatei **Dr.Web Antivirus für Windows** klicken Sie auf F1 im beliebigen Scanner-Fenster. Um die Kontexthilfe über einen Fensterbereich zu erhalten, klicken Sie mit der rechten Maustaste darauf.



Kapitel 5. Quarantäne

Um den Inhalt der **Quarantäne** anzuschauen und zu bearbeiten, wählen Sie den Menüpunkt **Quarantäne** im Kontextmenü des **Agenten** aus. Dabei öffnet sich ein Fenster mit den in Form von Tabelle dargestellten Daten über den aktuellen Status der **Quarantäne**.

Die **Quarantäne** von **Dr.Web** Antivirus dient zur Isolation von verdächtigen Dateien, die Schadprogramme enthalten können.

Ein **Quarantäne**-Ordner wird auf jeder Festplatte erstellt, wo verdächtige Dateien entdeckt wurden. Der **Quarantäne**-Ordner, der `DrWeb Quarantine` genannt wird, wird im Root der Festplatte erstellt und gehört zu versteckten Ordnern. Der Benutzer hat keine Zugriffsrechte auf die Dateien im **Quarantäne**-Ordner.

Bei Entdeckung von infizierten Objekten auf einem Wechseldatenträger wird der Ordner `DrWeb Quarantine` nur dann erstellt, wenn das Schreiben auf den Wechseldatenträger möglich ist. Das infizierte Objekt wird in diesen Ordner verschoben.



Die **Quarantäne**-Dateien, die auf einer Festplatte untergebracht werden, werden verschlüsselt gespeichert.

Die **Quarantäne**-Dateien, die auf einem Wechseldatenträger untergebracht werden, werden nicht verschlüsselt.





Es ist erforderlich, dass die Stations mit dem installierten **Quarantäne**-Modul unter Betriebssystemen funktionieren, auf welchen **SpIDer Guard G3** installiert werden kann (s. Punkt Systemanforderungen).

Im Gegenfall wird die **Quarantäne** nicht imstande sein, die Dateien aus dem Ordner `Infected.!!!` zu verwalten (dieser Ordner befindet sich im Antivirus-Installationsordner) und die Information über den **Quarantäne**-Inhalt wird dem **Server** nicht zugesandt.

5.1. Benutzeroberfläche einstellen

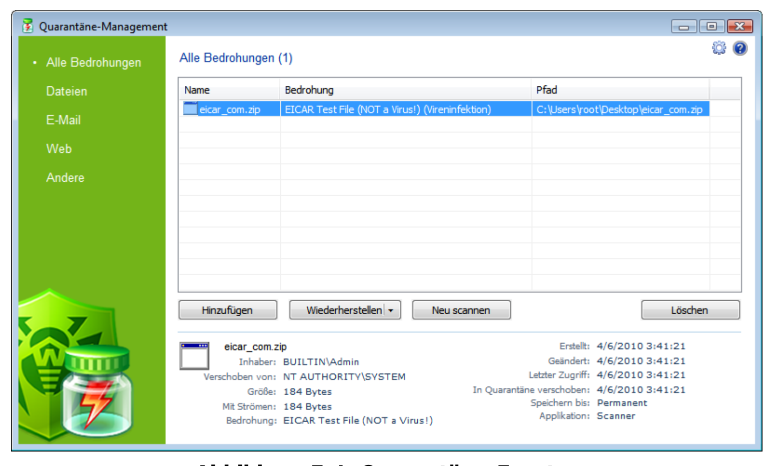


Abbildung 5-1. Quarantäne-Fenster

Im zentralen Fensterbereich wird die Objekt-Tabelle mit der Information über den Status der Quarantäne angezeigt. Standardmäßig besteht die Tabelle aus folgenden Spalten:

- **Name** – Liste der Namen von Objekten in Quarantäne,
- **Bedrohung** – Klasse des Schadprogramms, die vom **Antivirus** bei automatischer Übertragung des Objektes in die Quarantäne bestimmt wird,



- **Pfad** – Vollständiger Pfad des Objektes vor seiner Verschiebung in **Quarantäne**.

Es ist auch möglich, die Darstellung von Spalten mit ausführlicher Information über das Objekt einzustellen. Diese Information ist den Daten im unteren Fensterbereich der **Quarantäne** ähnlich.

Um die Darstellung der Spalten einzustellen:

1. Rufen Sie das Header-Kontextmenü der Objekt-Tabelle auf. Dafür klicken Sie mit der rechten Maustaste auf den Header.
2. Im Kontextmenü wählen Sie **Spalten anpassen** aus.
3. Im geöffneten Fenster setzen Sie Häkchen bei den Punkten, die Sie in die Objekt-Tabelle einschließen möchten. Um die Spalten aus der Objekt-Tabelle auszuschließen, entfernen Sie die Häkchen bei entsprechenden Punkten.
   a) Um Häkchen bei sämtlichen Objekten gleich zu setzen, klicken Sie auf **Alles markieren**.
   b) Um alle Häkchen zu entfernen, klicken Sie auf **Markierung aufheben**.
4. Um die Folge der Spalten in der Tabelle zu ändern, wählen Sie die entsprechende Spalte in der Liste aus und klicken Sie auf einen der folgenden Knöpfe:
   a) **Nach oben** – zur Verschiebung der Spalte in Richtung zum Tabellenanfang (d.h. aufwärts in der Liste der Einstellungen und nach links in der Objekt-Tabelle).
   b) **Nach unten** – zur Verschiebung der Spalte in Richtung zum Tabellenende (d.h. abwärts in der Liste der Einstellungen oder nach rechts in der Objekt-Tabelle).
5. Um die Änderungen in den Einstellungen zu speichern, klicken Sie auf **OK**. Um das Fenster zu schließen, ohne dabei die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Im unteren Bereich des **Quarantäne**-Fensters wird ausführliche Information über ausgewählte Objekte in **Quarantäne** angezeigt.



5.2. Eigenschaften der Quarantäne einstellen

Um die Eigenschaften der Quarantäne einzustellen:

1. Klicken Sie auf den Knopf **Einstellungen** im **Quarantäne**-Fenster.
2. Es öffnet sich dabei das Fenster **Quarantäne-Eigenschaften,** in dem folgende Parameter geändert werden können:
   - Abschnitt **Quarantäne-Größe definieren** ermöglicht die Verwaltung des Festplattenspeicherplatzes, der vom **Quarantäne**-Ordner gefüllt wird. Verschieben Sie den Regler, um die maximal zulässige Größe der **Quarantäne** zu ändern. Die maximal zulässige Größe der Quarantäne wird im Prozentanteil hinsichtlich der gesamten Festplattengröße bestimmt (falls mehrere Festplatten vorhanden sind, wird dieser Wert für jede einzelne Festplatte, auf der die **Quarantäne**-Ordner untergebracht werden, berechnet). `100%` bedeutet, dass die Einschränkungen für den maximalen Speicherplatz des **Quarantäne**-Ordners aufgehoben werden.
   - Im Abschnitt **Anzeigen** setzen Sie ein Häkchen bei **Backup-Dateien anzeigen**. Dabei werden die Reservekopien der Dateien, die sich in **Quarantäne** befinden, in der Objekt-Tabelle angezeigt.
3. Nachdem das Bearbeiten der Einstellungen abgeschlossen wird, klicken Sie auf **OK**, um die ausgeführten Änderungen zu speichern, oder auf **Abbrechen**, um sich auf Änderungen zu verzichten.

Die Reservekopien werden automatisch bei Verschiebung der Dateien in **Quarantäne** erstellt. Wenn auch die Dateien in **Quarantäne** **unbefristet** gespeichert werden, werden deren Reservekopien nur **temporär** gespeichert (s. auch Abschnitt Bereinigung der Quarantäne).

Zur Anzeige der Hilfedatei klicken Sie auf .



5.3. Den Quarantäne-Inhalt verwalten

Die Seitenleiste links dient zur Filterung der **Quarantäne**-Objekte, die angezeigt werden. Beim Klicken auf den entsprechenden Punkt im mittleren Bereich des Fensters werden alle Objekte in **Quarantäne** oder nur bestimmte Objektgruppen angezeigt: Dateien, Mail-Objekte, Websites oder alle anderen Objekte, die keiner Gruppe zugeordnet werden.



Für die Benutzer sind die Dateien im **Quarantäne**-Ordner sichtbar, auf welche diese Besitzer Zugriffsrechte haben.

Um versteckte Objekte anzuzeigen, starten Sie entweder die im Installationsordner untergebrachte `dwqrui.exe` **Quarantäne**-Datei oder die Benutzeroberfläche des **Dr. Web Agenten** unter einem Benutzernamen, der über Administratorrechte verfügt (s. Punkt Benutzeroberfläche des Dr.Web Agenten starten und stoppen).

In dem **Quarantäne**-Fenster sind folgende Steuerungsknöpfe verfügbar:

- **Hinzufügen** – eine Datei in **Quarantäne** verschieben. Im geöffneten Datei-Browser wählen Sie nötige Datei aus.
- **Wiederherstellen** – eine Datei aus der **Quarantäne** verschieben und an ihrem ursprünglichen Platz auf dem Computer wiederherstellen (die Datei mit ihrem Namen in dem Ordner, in dem sie sich vor Verschiebung in **Quarantäne** befand, wiederherstellen).



Nutzen Sie diese Funktion nur in dem Fall, wenn Sie sicher sind, dass das Objekt zuverlässig ist.

Das ausfallende Menü verfügt über die Variante **Wiederherstellen in** – eine Datei unter dem angegebenen Namen in den Ordner, der vom Benutzer bestimmt wird, übertragen.

- **Neu scannen** – eine Datei in **Quarantäne** erneut scannen



lassen. Falls es sich beim Neuscannen der Datei zeigt, dass diese Datei nicht infiziert ist, wird es von der **Quarantäne** angeboten, diese Datei wiederherzustellen.

- **Löschen** – eine Datei aus der **Quarantäne** und aus dem Betriebssystem löschen.

Um gleichzeitig mit mehreren Objekten arbeiten zu können, wählen Sie die erforderlichen Objekte im **Quarantäne**-Fenster aus, indem Sie die Tasten SHIFT und CTRL gedrückt halten. Danach klicken Sie mit der rechten Maustaste auf beliebige Tabellenzeile und wählen Sie die erforderliche Aktion aus.

5.4. Bereinigung der Quarantäne

Automatische Bereinigung der Quarantäne

Bei Überfüllung der Festplatte wird eine automatische Bereinigung der Quarantäne ausgeführt:

1. In erster Reihe werden die Reservekopien der Dateien in **Quarantäne** gelöscht.
2. Wenn der Festplattenspeicherplatz nicht ausreicht, werden die Dateien in **Quarantäne**, deren Speicherdauer abgelaufen ist, gelöscht.



Wenn die **Quarantäne** überfüllt ist und es keine Möglichkeit besteht, sie automatisch zu entleeren, wird die Verschiebung der Dateien in **Quarantäne** mit Fehler beendet. In diesem Fall können Sie die **Quarantäne** im Abschnitt **Eigenschaften der Quarantäne** → **Größe der Quarantäne festsetzen** vergrößern oder die Dateien aus der **Quarantäne** per Hand löschen.



Quarantäne völlig bereinigen

Den ganzen Inhalt der Quarantäne können Sie folgenderweise löschen:

1. Öffnen Sie den **Quarantäne**-Manager über Kontextmenü des **Agenten**. Wählen Sie den Menüpunkt **Quarantäne** aus. Markieren Sie alle Dateien im **Quarantäne**-Fenster und klicken Sie auf **Löschen**.
2. Nutzen Sie die Systemfunktion **Disk Cleanup**, um Festplatte zu reinigen.

   Diese Funktion kann auf zwei Weisen gestartet werden:

   - Über Menü **Start** → **Programme** → **Zubehör** → **Systemprogramme** → **Datenträgerbereinigung**. Wenn es mehrere Datenträger vorhanden sind, wählen Sie den Datenträger, auf dem Sie die **Quarantäne** bereinigen möchten.
   - Über Datei-Browser des Betriebssystems: im Kontextmenü des lokalen Datenträgers, auf dem **Quarantäne** zu bereinigen ist, wählen Sie **Eigenschaften** → **Bereinigen** aus.

   Im geöffneten Fenster **Datenträgerbereinigung** setzen Sie ein Häkchen bei **Dr.Web Quarantäne** in der Liste **Zu löschende Dateien** und klicken Sie auf **OK**. Der ganze Inhalt der **Quarantäne** wird gelöscht.



Kapitel 6. Dr.Web Firewall

Dr.Web Firewall Netzwerkmonitor ist für den Schutz Ihres Computers vor unbefugtem Zugang von außen bestimmt und beugt dem Verlust wichtiger Daten im Netzwerk vor. Diese Komponente gestattet Ihnen die Kontrolle über die Verbindung und Übermittlung von Daten übers Internet sowie die Sperre von verdächtigen Verbindungen auf der Paket- und Anwendungsebene.

Nach der Installation von **Dr.Web Firewall** wird die Weiterbildung des Programms im Prozess Ihrer Arbeit am Computer einige Zeit lang durchgeführt. Die Beschreibung vom Trainingmodus des Netzwerkmonitors finden Sie in der Anleitung **Dr.Web Antivirus für Windows**, Abschnitt **Dr.Web Firewall Training**.

Für den Übergang zur Hilfedatei **Dr.Web Antivirus für Windows** klicken Sie auf F1 im beliebigen Fenster des Netzwerkmonitors.

Mit Hilfe vom Kontextmenü des **Agenten** können Sie:

1. Einstellungen des Netzwerkmonitors aufrufen.
2. Ereignis-Logdatei ansehen.

6.1. Dr.Web Firewall Einstellungen

Zum Ansehen und Bearbeiten der Parameter vom **Dr.Web Firewall** Netzwerkmonitor wählen Sie den Menüpunkt **Firewall-Einstellungen** im Kontextmenü des **Agenten** aus.



Der Menüpunkt **Firewall-Einstellungen** ist im Kontextmenü des **Agenten** nur zugänglich, wenn der Benutzer Administratorrechte auf diesem Computer besitzt.

Es öffnet sich das Fenster mit Einstellungen von **Dr.Web Firewall**. Ausführliche Beschreibung des Verwaltungsvorganges für die **Dr.Web Firewall** Komponente finden Sie in der Anleitung **Dr.Web Antivirus**



für Windows, Abschnitt **Firewall Einstellungen**.

Für den Übergang zur Hilfedatei **Dr.Web Antivirus für Windows** klicken Sie auf F1 im beliebigen Fenster des Netzwerkmonitors.

6.2. Dr.Web Firewall Log

Um den Log des Netzwerkmonitors von **Dr.Web Firewall** anzuschauen, wählen Sie den Menüpunkt **Firewall-Protokoll** im Kontextmenü des **Agenten** aus.



Der Menüpunkt **Firewall-Protokoll** ist im Kontextmenü des **Agenten** nur zugänglich, wenn der Besitzer Administratorrechte auf diesem Computer besitzt.

Es öffnet sich das Fenster vom **Dr.Web Firewall** Log. Ausführliche Beschreibung des **Dr.Web Firewall** Logs finden Sie in der Anleitung **Dr.Web Antivirus für Windows**, Abschnitt **Protokollieren der Ereignisse**.

Für den Übergang zur Hilfedatei **Dr.Web Antivirus für Windows** klicken Sie auf F1 im beliebigen Fenster des Netzwerkmonitors.



Kapitel 7. Office Kontrolle

Das Modul der **Office Kontrolle** von **Dr.Web** beschränkt den Benutzerzugriff auf bestimmte lokale Ressourcen und Websites. Dies gewährleistet nicht nur die Kontrolle über die Integrität wichtiger Dateien und deren Schutz vor Vireninfizierung sondern auch die Bewahrung des Datengeheimnisses auf Ihrem Computer.

Es besteht die Möglichkeit, sowohl einzelne Dateien als auch komplette Ordner, die sich auf lokalen Datenträgern oder Wechseldatenträgern (solange deren Verbindung zum Computer besteht) befinden, zu schützen. Darüber hinaus kann ein vollständiges Verbot auf die Anzeige der Informationen von allen externen Datenträgern verhängt werden.

Die Verwaltung des Zugriffs auf Internetressourcen ermöglicht dem Benutzer sowohl den Schutz vor unerwünschten Websites (wo es sich um Gewalt, Glücksspiele usw. handelt) als auch einen kontrollierten Zugriff auf die vom Benutzer durch **Office Kontrolle** definierten Internetseiten.

Standardmäßig blockiert der Wächter den Zugriff auf die **Dr.Web** Antivirus-Ordner. Um die Parameter für die Funktion des Moduls festzusetzen, verwenden Sie die entsprechenden Einstellungen.

Je nach Parametern auf dem **Server** können Sie das Modul der **Office Kontrolle** einstellen.



Neben der Möglichkeit, den Zugang auf Inhalte seitens Benutzers einzuschränken, wird auch die Möglichkeit, Einstellungen auf dem **Server** durch Administrator festzusetzen, aufbewahrt. Die auf dem **Server** angegebenen Einstellungen werden seitens Benutzers automatisch aktualisiert.

Um die Einstellungen des Moduls zu ändern:

1. Wählen Sie den Menüpunkt **Office Control Einstellungen** im Kontextmenü des Agenten aus.





Der Menüpunkt **Office Control Einstellungen** ist im Kontextmenü des **Agenten** nur zugänglich, wenn der Benutzer:

1. Rechte, die diese Einstellungen ändern lassen, besitzt. Die Rechte werden vom Administrator des Antivirus-Netzwerkes auf dem **Server** festgesetzt.
2. Administratorrechte auf diesem Computer besitzt.

2. Geben Sie das Passwort für den Zugang auf das Modul der **Office Kontrolle** ein.



Der Schutz vor Editierung der Ressourcen-Liste erfolgt mit einem Passwort, das bei erster Einstellung des Moduls der **Office Kontrolle** festgesetzt wird. Sie können das Passwort im Einstellungsfenster des Moduls ändern oder sich dafür an Administrator wenden.

Um das Passwort zu ändern, klicken Sie auf den Knopf **Passwort ändern**, der sich im Einstellungsfenster befindet.

3. Um Information über die Einstellungen im Tab zu erhalten, klicken Sie auf (**Hilfe**).
4. Nehmen Sie benötigte Änderungen in den Einstellungstabs vor:
   - **URL-Filter** (ausführliche Beschreibung finden Sie in der Hilfedatei **Dr.Web Antivirus für Windows**, Abschnitt **URL-Filter**).
   - **Lokalzugriff** (ausführliche Beschreibung finden Sie in der Hilfedatei **Dr.Web Antivirus für Windows**, Abschnitt **Lokaler Zugriff**).

   Für den Übergang zur Hilfedatei **Dr.Web Antivirus für Windows** klicken Sie auf F1 im beliebigen Fenster der **Office Kontrolle**.
5. Klicken Sie auf **Anwenden**, um die ausgeführten Änderungen zu speichern, ohne dabei das Einstellungsfenster zu schließen.

6. Nachdem die Bearbeitung von Einstellungen beendet wird, klicken Sie auf **OK**, um alle ausgeführten Änderungen zu speichern, oder auf **Abbrechen**, um das Einstellungsfenster ohne Speicherung von Änderungen zu schließen.



Kapitel 8. SpIDer Gate

Der HTTP-Wächter **SpIDer Gate** hilft Ihnen, Ihren Computer vor Schadprogrammen, die sich beim Zusammenwirken im Netzwerk über HTTP-Protokoll verbreiten können, zu schützen. Über HTTP funktionieren die Web-Browsers (Internet-Browsers), unterschiedliche Download-Manager und mehrere andere Programme, die Daten im Internet erhalten. Solche Programme werden auch HTTP-Clients genannt.

Standardmäßig gehört **SpIDer Gate** zum Umfang der zu installierenden Komponenten. Dieses Modul läuft regelmäßig im Speicher und wird beim Neustarten von Windows automatisch gestartet.

Durch die Änderung der Einstellungen von **SpIDer Gate** können Sie die Prüfung des ausgehenden oder eingehenden Verkehrs deaktivieren sowie die Liste von Anwendungen, deren HTTP-Verkehr(Information, die über HTTP-Protokoll übertragen wird) auf jeden Fall im vollen Umfang zu prüfen ist, erstellen. Es besteht auch die Möglichkeit, manche Anwendungen von der Prüfung auszschließen.

Die Parameteränderung von der mit dem **SpIDer Gate** HTTP-Wächter auszuführenden Prüfung kann vom Administrator von **Dr.Web Enterprise Security Suite** freigegeben oder blockiert werden. Zum Ansehen und Bearbeiten von Parametern des **SpIDer Gate** HTTP-Wächters wählen Sie den Menüpunkt **SpIDer Gate Einstellungen** im Kontextmenü des **Agenten** aus.



Der Menüpunkt **SpIDer Gate Einstellungen** ist im Kontextmenü des **Agenten** nur zugänglich, wenn der Benutzer:

1. Rechte, die diese Einstellungen ändern lassen, besitzt. Die Rechte werden vom Administrator des Antivirus-Netzwerkes auf dem **Server** festgesetzt.
2. Administratorrechte auf diesem Computer besitzt.



Standardmäßig wird der ganze HTTP-Verkehr vom Wächter geprüft. Die Prüfungsparameter können Sie die mit Hilfe von entsprechenden Modul-Einstellungen festsetzen.

Mehr zur Verwaltung des **SpIDer Gate** Wächters finden Sie in der Anleitung **Dr.Web Antivirus für Windows**, Abschnitt **SpIDer Gate Einstellung**.

Für den Übergang zur Hilfedatei **Dr.Web Antivirus für Windows** klicken Sie auf F1 im beliebigen Fenster des Wächters.

Kapitel 9. SpIDer Guard

SpIDer Guard ist ein Antiviruswächter (auch Dateimonitor genannt). Das Programm läuft permanent im Hauptspeicher des Computers. Der Wächter prüft Dateien "on the fly" und entdeckt eventuelle Virenaktivitäten.

SpIDer Guard wird automatisch bei jedem Start des Betriebssystems aktiviert. Der automatisch aktivierte Wächter kann dabei innerhalb der laufenden Sitzung des Betriebssystems nicht deaktiviert werden. Im Bedarfsfall (z. B. bei der Ausführung einer für die Prozessorauslastung kritischen Aufgabe im Echtzeitmodus) können Sie das "on the fly" Scannen von Dateien temporär ausschalten.

Nach Voreinstellungen überprüft **SpIDer Guard** "on the fly" alle Dateien, die erstellt oder geändert werden, sowie die Bootsektoren. Auf Wechseldatenträgern und Netzwerklaufwerkn werden auch alle geöffneten Dateien geprüft. Dabei wird jede Datei ähnlich wie vom **Dr. Web Scanner** überprüft, aber unter "milderen" Überprüfungsbedingungen. Außerdem verfolgt der **SpIDer Guard** Wächter permanent die Aktionen der gestarteten Vorgänge, die für Viren charakteristisch sind, und blockiert sie, wenn Sicherheitsbedrohungen entdeckt werden.

Bei Entdeckung infizierter Objekte nimmt **SpIDer Guard** Wächter Aktionen vor, die den vordefinierten Einstellungen entsprechen. Durch die entsprechende Veränderung von Einstellungen können Sie automatische Reaktion des Programms auf Virenereignisse bestimmen.

Wächter einstellen

Der Einstellungsabschnitt vom **SpIDer Guard** Wächter unterscheidet sich je nach Version des installierten Programms. Vorhanden sind zwei Versionen des **SpIDer Guard** Wächters:

- SpIDer Guard G3,
- SpIDer Guard NT4.



Vor Installation des Wächters wird die Version des Betriebssystems automatisch bestimmt. Dementsprechend wird die Version des **SpIDer Guard** Wächters installiert (s. Punkt Systemanforderungen).

9.1. SpIDer Guard G3 Einstellungen



Die Einstellungen des Standardprogramms sind für die meisten Anwendungen optimal und sind ohne Not nicht zu verändern.

Um SplDer Guard Dateimonitor einzustellen:

1. Im Kontextmenü des **Agenten** wählen Sie den Menüpunkt **SpIDer Guard Einstellungen** aus.



Der Menüpunkt **SpIDer Guard Einstellungen** ist im Kontextmenü des **Agenten** nur zugänglich, wenn der Benutzer:

1. Rechte, die diese Einstellungen ändern lassen, besitzt. Die Rechte werden vom Administrator des Antivirus-Netzwerkes auf dem **Server** festgesetzt.
2. Administratorrechte auf diesem Computer besitzt.

2. Es öffnet sich das Einstellungsfenster mit folgenden Abschnitten:
   - Abschnitt Allgemein, in dem der Prüfungsmodus für Dateien und Vorgänge des zu schützenden Computers konfiguriert wird.
   - Abschnitt Aktionen, in dem die Reaktion des **SpIDer Guard** Wächters bei Entdeckung infizierter oder verdächtiger Dateien sowie Malware konfiguriert wird.
   - Abschnitt Ausgenommen, in dem eine Liste der vom Scannen durch den **SpIDer Guard** Wächter ausgeschloßenen Ordner und Dateien konfiguriert wird.

- Abschnitt Protokoll, in dem der Modus der Protokolldateiführung des **SpIDer Guard** Wächters konfiguriert wird.

3. Nehmen Sie die erforderlichen Änderungen vor.
4. Nach der Bearbeitung der Einstellungen, klicken Sie auf **OK**, um die ausgeführten Änderungen zu speichern, oder auf **Abbrechen**, um sie aufzugeben.



Um Information über das aktive Einstellungsfenster von **SpIDer Guard** zu erhalten, klicken Sie auf F1. Um Kontexthilfe über einen Fensterbereich zu erhalten, klicken Sie mit der rechten Maustaste darauf.



9.1.1. Allgemein

SpIDer Guard G3 Einstellungen - Dr.Web Antivirus

Allgemein | Aktionen | Ausgenommen | Protokoll

- [x] Heuristische Analyse
- [x] Laufende Anwendungen und Module prüfen

Prüfen: Beim Programmstart

- [x] Dateien nach dem Update der Virendatenbanken neu prüfen
- [x] Optimaler Modus
- [x] Autorun von Wechseldatenträgern blockieren
- [x] Wechseldatenträger prüfen
- [ ] Dateien im Netzwerk prüfen

OK | Cancel

Abbildung 9-1. Einstellungsfenster von SpIDer Guard. Tab Allgemein. Um Info über die Parameter in einem anderen Tab zu erhalten, klicken Sie auf entsprechenden Tabnamen in der Abbildung

Im Tab **Allgemein** wird der Prüfungsmodus der Dateien und Prozesse des geschützten Compuetrs konfiguriert:



- Setzen Sie ein Häkchen bei **Heuristische Analyse**, um den heuristischen Analysator bei der Prüfung zu verwenden.

  Entfernen Sie das Häkchen, um die Prüfung nur aufgrund bekannter Virensignaturen durchzuführen (s. auch Abschnitt Entdeckungsverfahren von Viren).

- Die Option **Laufende Anwendungen und Programme prüfen** lässt die Dateien von Programmen, die zu diesem Zeitpunkt aktiv sind, prüfen. Um den Prüfungsmodus für Dateien der ausführbaren Vorgänge zu konfigurieren, wählen Sie in der ausfallenden Liste eine der folgenden Varianten aus:
  - **im Hintergrundmodus** - die Module werden im Hintergrundmodus geprüft, d.h. nachdem sie gestartet und während sie ausgeführt werden.
  - **beim Programmstart** - die Module werden vor ihrem Starten geprüft.
- Wird ein Häkchen bei **Dateien nach dem Update der Virendatenbanken neu prüfen** gesetzt, so werden alle aktiven, zu diesem Zeitpunkt geladene Module und infizierte Dateien gleich nach der Aktualisierung der Virendatenbanken wiederholt geprüft. Wenn dieses Häkchen entfernt wird, so werden nur die infizierten Dateien nach der Aktualisierung der Virendatenbanken neu geprüft.
- Das Häkchen bei **Optimaler Modus** regelt den Prüfungsmodus, in dem es festgesetzt wird, bei welchen Aktionen ein Objekt vom **SpIDer Guard** Wächter geprüft werden soll:
  - Wird ein Häkchen bei **Optimaler Modus** gesetzt, so werden die Dateien auf Festplatten nur bei manchen Zugriffen darauf gescannt: wenn sie für Ausführung gestartet werden, beim Erstellen, beim Schreiben (beim Versuch zu schreiben) in die bestehenden Dateien und Bootsektoren.
  - Wird kein Häkchen bei **Optimaler Modus** gesetzt, so werden die Dateien auf Festplatten bei sämtlichen Zugriffen darauf gescannt: wenn sie für Ausführung gestartet werden, beim Erstellen, beim Schreiben (beim Versuch zu schreiben) in die bestehenden Dateien und Bootsektoren sowie beim beliebigen Öffnen der Dateien, einschließlich der Dateien nur zum Lesen.



Beim Deaktivieren des **Optimaler Modus** wird der maximale Schutz sichergestellt, dabei aber wird die Belastung des Computers wesentlich steigen.

Die Prüfungsmodi für Dateien auf Wechseldatenträgern und auf Netzwerklaufwerken werden separat mit Häkchen bei **Wechseldatenträger prüfen** und **Dateien im Netzwerk prüfen** konfiguriert.

Präzisierungen und Empfehlungen

Es wird empfohlen, den **Optimaler Modus** nur nach einer sorgfältigen Prüfung aller Festplatten unter Anwendung von **Dr.Web Scanner** zu nutzen. Dabei wird das Eindringen neuer Viren und anderer schädlichen Programme auf den Computer über die Wechselmedien verhindert. Es wird jedoch hierbei kein wiederholtes Scannen der bereits geprüften, "sauberen" Objekte durchgeführt.

Die Reaktion des **SpIDer Guard** Wächters auf die Entdeckung schädlicher Objekte wird im Abschnitt Aktionen konfiguriert.



Manche externe Speicher (insbesondere externe Festplatten mit USB-Schnittstelle) können im Betriebsystem als Festplatten angezeigt werden. Deswegen sollen solche Geräte unter besonderer Vorsicht genutzt und beim Anschließen an Computer auf Viren unter Anwendung von **Dr.Web Scanner** geprüft werden.

- Das Häkchen bei **Autorun von Wechseldatenträgern blockieren** verbietet das automatische Starten der Programme von externen Datenträgern. Somit werden Sie Ihren Computer vom Starten der Schadprogramme, die sich auf externen Datenträgern befinden können, schützen.
- Setzen Sie ein Häkchen bei **Wechseldatenträger prüfen**, um die Dateien auf den Wechseldatenträgern (CD/DVD, Magnetplatten (FDD), flash-Speicher und sonstige Datenträger, die über einen USB-Port angeschlossen werden) bei beliebigem Zugriff darauf, eingeschlossen vom Öffnen der Dateien nur zum Lesen, zu scannen.



Wird das Häkchen bei **Wechseldatenträger prüfen** entfernt, so werden die Dateien auf den Wechseldatenträgern nur gescannt, wenn die Ausführung solcher Dateien angefordert wird.

- Setzen Sie ein Häkchen bei **Dateien im Netzwerk prüfen**, um Objekte auf Netzwerklaufwerken zu scannen, falls deren Ausführung auf Ihrem Computer angefordert wird sowie beim beliebigen Öffnen der Dateien, eingeschlossen von Dateien nur zum Lesen.

  Wird das Häkchen bei **Dateien im Netzwerk prüfen** entfernt, so werden die Dateien auf den Netzwerklaufwerken nur gescannt, wenn die Ausführung solcher Dateien auf Ihrem Computer angefordert wird.



9.1.2. Aktionen

SpIDer Guard G3 Einstellungen - Dr.Web Antivirus

Allgemein | Aktionen | Ausgenommen | Protokoll

Adware: In Quarantäne
Dialer: Löschen
Scherzprogramme: Löschen
Riskware: Benachrichtigen
Hackertools: Benachrichtigen
Infiziert: Desinfizieren
Verdächtig: In Quarantäne
Nicht desinfizierbar: In Quarantäne
Installationspakete prüfen
Installationspakete: In Quarantäne

OK | Cancel

Abbildung 9-2. Einstellungsfenster von SpIDer Guard. Tab Aktionen. Um Info über die Parameter in einem anderen Tab zu erhalten, klicken Sie auf entsprechenden Tabnamen in der Abbildung

Im Tab Aktionen wird die Reaktion des **SpIDer Guard** Wächters bei Entdeckung infizierter oder verdächtiger Dateien und Schadprogramme konfiguriert. Die zugänglichen Reaktionen unterscheiden sich je nach dem Typ des Virenereignisses.



Folgende Aktionen können für gefundene Objekte ausgeführt werden:

- **Desinfizieren** - den Zustand des infizierten Objektes vor seiner Infizierung wiederherstellen. Wenn das Desinfizieren unmöglich ist, wird die Einstellung für nicht desinfizierbare Objekte verwendet.

  Diese Aktion ist nur für die mit bekannten desinfizierbaren Viren infizierten Objekte möglich. Ausgenommen sind Trojaner und infizierte Dateien innerhalb der zusammengesetzten Objekte (Archive, E-Mail-Dateien oder Datei-Container).

- **Löschen** - infizierte Objekte löschen.
- **In Quarantäne** - infizierte Objekte in den Quarantäne-Ordner verschieben.
- **Benachrichtigen** - nur eine Benachrichtigung bei Virenfund senden (mehr zur Einstellung des Benachrichtigungsmodus s. unten).
- **Ignorieren** - das Objekt ohne Anwendung jeglicher Aktionen und ohne Benachrichtigung überspringen.



Wird die Aktion **Ignorieren** ausgewählt, werden keine Aktionen ausgeführt: im Gegensatz zur aktivierten Option **Benachrichtigen** erhält der Benutzer keine Benachrichtigung bei Entdeckung eines schädlichen Objektes.

Tabelle 3. SpIDer Guard Aktionen bei entdeckten schädlichen Objekten

Objekt	Aktion				
	Desinfizieren	Löschen	In Quarantäne	Benachrichtigen	Ignorieren
Adware		+	+/*	+	+
Dialer		+	+	+/*	+
Scherzprogramme		+/*	+	+	+
Riskware		+	+	+/*	+



Objekt	Aktion				
	Desinfizieren	Löschen	In Quarantäne	Benachrichtigen	Ignorieren
Hackertools		+	+	+/*	+
Infiziert	+/*	+	+		
Verdächtig		+	+/*	+	+
Nicht desinfizierbar		+	+/*		
Installationspakete		+	+/*	+	+

Symbole

+	Die Aktion ist für diesen Typ der Objekte freigegeben
+/*	Die Aktion ist als standardmäßige Reaktion für diesen Typ der Objekte festgesetzt

Zur Festsetzung der Aktionen für entdeckte schädliche Objekte werden folgende Einstellungen verwendet:

- Die ausfallende Liste **Adware** setzt die Reaktion von **SpIDer Guard** auf Entdeckung von diesem Typ der unerwünschten Software fest.
- Gleich der Reaktion auf Adware wird die Reaktion von **SpIDer Guard** auf Entdeckung von sonstigen unerwünschten Programmen eingestellt:
  - Dialer;
  - Scherzprogramme;
  - Riskware;
  - Hackertools.
- Die ausfallende Liste **Infiziert** setzt die Reaktion von **SpIDer Guard** auf Entdeckung einer Datei, die mit einem bekannten Virus infiziert ist.
- Die ausfallende Liste **Verdächtig** setzt die Reaktion von **SpIDer Guard** auf Entdeckung einer Datei, die mit einem Virus vermutlich infiziert ist (Ergebnis der heuristischen Analyse).
- Die ausfallende Liste **Nicht desinfizierbar** setzt die Reaktion



von **SpIDer Guard** auf Entdeckung einer Datei, die mit einem bekannten, nicht desinfizierbaren Virus infiziert ist (eingeschlossen der Desinfektionsversuche, die fehlgeschlagen sind).

- Die Option **Installationspakete prüfen** regelt die „on the fly“ Prüfung der Installationsdateien.

  Bei Einstellung dieser Option wählen Sie in der ausfallenden Liste **Installationspakete** eine Aktion, die bei Entdeckung der böswilligen Objekte in den Installationspaketen ausgeführt wird, aus.

Benachrichtigungen einstellen

Nach der Ausführung der vorgeschriebenen Aktion wird der **SpIDer Guard** Wächter standardmäßig eine Benachrichtigung im Infobereich von Windows anzeigen. Sie können die Anzeige von Benachrichtigungen erlauben oder verbieten.

Bei der Einstellung von Benachrichtigungen des **SpIDer Guard** Wächters setzen oder entfernen Sie ein Häkchen bei **Benachrichtigungen bei Virenfund** in der ausfallenden Liste **Einstellungen** im Kontextmenü des **Agenten**-Icons, um den Empfang dieser Meldungen freizugeben oder zu verbieten.



9.1.3. Ausgenommen

SpIDer Guard G3 Einstellungen - Dr.Web Antivirus

Allgemein | Aktionen | Ausgenommen | Protokoll

- [x] Systemdateien von der Prüfung auslassen
  - [ ] Prefetcher-Datenbankdateien auslassen
  - [ ] Windows Search Datenbank-Dateien auslassen

Ausgenommene Verzeichnisse und Dateien

... | Hinzufügen | Löschen

OK | Cancel

Abbildung 9-3. Einstellungsfenster von SpIDer Guard. Tab Ausgenommen.

Um Info über die Parameter in einem anderen Tab zu erhalten, klicken Sie auf entsprechenden Tabnamen in der Abbildung

Im Tab **Ausgenommen** wird die Liste der Ordner und Dateien, die vom Prüfungsvorgang durch den **SpIDer Guard** Wächter ausgenommen werden.



Das Häkchen **Systemdateien von der Prüfung auslassen** regelt die Ausnahme von Systemdateien, die zur inneren Liste der **SpIDer Guard** Komponente gehören, von der Prüfung. Diese Liste wird für jede Version von Windows aufgrund von Microsoft® Empfehlungen bezüglich Verwendung der Antivirus-Software erstellt.

Beim Setzen eines Häkchens bei **Systemdateien von der Prüfung auslassen** sind folgende Einstellungen zugänglich:

- Das Häkchen bei **Prefetcher-Datenbankdateien auslassen** setzt die Ausnahme der Datenbankdateien von Prefetcher (Komponente des Betriebssystems Microsoft Windows, die seinen Bootsvorgang fördert sowie die Startzeit der Programme dank der Speicherung von Information, die beim Laden benutzt wird, reduziert)-Systemkomponente von der Prüfung fest.
- Das Häkchen bei **Windows Search Datenbank-Dateien auslassen** regelt die Ausnahme der Datenbank-Dateien des Windows Search-Dienstes von der Prüfung.

In dem Abschnitt **Ausgenommene Verzeichnisse und Dateien** finden Sie eine Auflistung von Verzeichnissen und Dateien, welche von der Prüfung mit dem **SpIDer Guard** Wächter ausgeschlossen werden. Dies können die **Quarantäne**-Ordner des Antivirus, Arbeitsordner mancher Programme, temporäre Dateien (Swap-Dateien) u.ä. sein.

Standardgemäß ist die Liste leer. Sie können sowohl bestimmte Ordner und Dateien zu den Ausnahmen hinzufügen, als auch Masken verwenden, um die Prüfung von bestimmten Objektgruppen zu verbieten.

Ausnahmenliste erstellen

1. Um einen Ordner oder eine Datei zur Ausnahmenliste hinzuzufügen, führen Sie eine der folgenden Aktionen aus:
   - um einen bestimmten bestehenden Ordner oder eine Datei anzugeben, klicken Sie auf den <...> Knopf und wählen Sie einen Ordner oder eine Datei im standardmäßigen Betriebssystem-Browser aus. Außerdem können Sie den kompletten Pfad der Datei oder des Ordners manuell im Eingabefeld angeben;



- um alle Dateien oder Ordner mit einem bestimmten Namen von der Prüfung auszunehmen, geben Sie diesen Namen in das Eingabefeld ein. Die Angabe des Pfades zur Datei oder zum Ordner ist in diesem Fall nicht erforderlich;
- um die Dateien oder Ordner einer bestimmten Art von der Prüfung auszunehmen, geben Sie eine diese Objekte definierende Maske in das Eingabefeld ein.

Mehr zu Masken

Eine Maske setzt das Template für die Definition des Objektes fest. Sie kann sowohl übliche Zeichen, die für Dateinamen erlaubt sind, als auch spezielle Bezeichnungen beinhalten:

- `*` ersetzt eine beliebige (darunter auch leere) Folge beliebiger Zeichen;
- `?` ersetzt ein beliebiges Zeichen in bestimmter Position.

Beispiele:

- **bericht*.doc** – Maske, die alle Dokumente von Microsoft Word definiert, deren Name mit der bericht-Zeichenfolge anfängt, z.B. die Dateien `bericht-februar.doc`, `bericht121209.doc` usw.;
- ***.exe** – Maske, die alle ausführbaren Dateien mit der EXE Erweiterung definiert, z.B. setup.exe, iTunes.exe usw.;
- **photo????09.jpg** – Maske, die alle Dateien von JPG Bildern definiert, deren Name mit der photo Zeichenfolge anfängt und mit der Zeichenfolge `09` endet, wobei der Dateiname vier beliebige Zeichen zwischen den angegebenen Zeichenfolgen enthält, z.B. `photo121209.jpg`, `photomama09.jpg` oder `photo----09.jpg`.

2. Klicken Sie auf **Hinzufügen**.
3. Bei Bedarf wiederholen Sie die Schritte 1 und 2, um andere Dateien oder Ordner hinzuzufügen. Um eine Datei oder einen Ordner aus der Liste der Ausnahmen zu entfernen, wählen Sie das entsprechende Element in der Liste aus und klicken Sie auf **Löschen**.



9.1.4. Protokoll

Abbildung 9-4. Einstellungsfenster von SpIDer Guard. Tab Protokoll. Um Info über die Parameter in einem anderen Tab zu erhalten, klicken Sie auf entsprechenden Tabnamen in der Abbildung

Im Tab **Protokoll** wird der Modus der Protokollführung festgesetzt und Information angegeben, die in die Protokolldatei eingetragen wird.

Das Protokoll des **SpIDer Guard** Wächters wird in der `spiderg3.log` Protokolldatei gespeichert. Diese befindet sich im Installationsordner von **Dr.Web Enterprise Security Suite**.



Es empfiehlt sich, die Protokolldatei regelmäßig zu analysieren.

Zur Detaillierung des Protokolls setzen Sie Häkchen bei Modi für Protokollführung und Typen der Information, die ins Protokoll gehört.

Um die Modi für Protokollführung einzustellen, werden folgende Häkchen gesetzt:

- **Detailliertes Protokoll** – außer allgemeinen Ereignissen werden die ausführlichen Daten über geprüfte Objekte in diesem Protokollmodus erfasst. Es wird empfohlen, diesen Modus für die Definition der Objekte zu nutzen, deren Prüfung vom **SpIDer Guard** Wächter am häufigsten durchgeführt wird. Bei Bedarf können Sie solche Objekte auch in die Liste der Ausnahmen eintragen, was die Belastung des Computers reduzieren kann.
- **Debug-Protokoll** – in diesem Protokollmodus wird der maximale Informationsumfang über die Funktion des **SpIDer Guard** Wächters im Protokoll erfasst, was zu einer erheblichen Vergrößerung der Protokolldatei führen kann. Die Nutzung dieses Modus wird nur bei Schwierigkeiten im Betrieb des **SpIDer Guard** Wächters oder auf Verlangen des technischen Support-Dienstes von **Dr.Web** empfohlen.

Um die Typen der Information, die im Protokoll erfasst wird, festzusetzen, werden folgende Häkchen gesetzt:

- **Packprogramm ausführbarer Dateien anzeigen** - regelt die Eintragung der Meldungen über die Entdeckung von ausführbaren Dateien, die mit speziellen Packprogrammen verpackt wurden, sowie der Namen dieser Packprogramme. Standardmäßig wird dieses Häkchen nicht gesetzt.
- **Nicht infizierte Dateien** - regelt die Eintragung der Namen von allen geprüften Objekten, eingeschlossen von nicht infizierten Objekten mit einem `Ok` Vermerk (in diesem Modus



kann die Protokolldatei wesentlich größer werden). Standardmäßig wird dieses Häkchen nicht gesetzt.

- **Archiver anzeigen** - regelt die Eintragung der Meldungen über geprüfte Archive und über Programme, mit denen diese Archive erstellt wurden, sowie über die damit verbundenen Fehler (z.B. Archiv wurde nicht entpackt, da es mit Passwort geschützt ist). Standardmäßig wird dieses Häkchen nicht gesetzt.

Das Feld **Maximale Größe der Protokolldatei** lässt die Größe der Protokolldatei einschränken, indem ihre maximal zulässige Größe in KB festgesetzt wird.

9.2. SpIDer Guard NT4 Einstellungen



Die Einstellungen des Standardprogramms sind für die meisten Anwendungen optimal und sind ohne Not nicht zu verändern.

Um SpIDer Guard NT4 Dateimonitor einzustellen:



Der Menüpunkt **SpIDer Guard Einstellungen** ist im Kontextmenü des **Agenten** nur zugänglich, wenn der Benutzer:

1. Rechte, die diese Einstellungen ändern lassen, besitzt. Die Rechte werden vom Administrator des Antivirus-Netzwerkes auf dem **Server** festgesetzt.
2. Administratorrechte auf diesem Computer besitzt.

1. Zum Ansehen oder Ändern der Scanparameter wählen Sie den Menüpunkt **SpIDer Guard Einstellungen** → **Scan-Einstellungen** im Kontextmenü des **Agenten** aus. Ausführliche Beschreibung der Einstellungen finden Sie im Punkt Scan-Einstellungen.
2. Um die Start-Parameter des Wächters, seine Einstellungen und Benachrichtigungen über Ereignisse anzuschauen oder zu ändern, wählen Sie den Menüpunkt **SpIDer Guard Einstellungen** → **Verwaltung** im Kontextmenü des



Agenten aus. Ausführliche Beschreibung der Verwaltung finden Sie im Abschnitt Verwaltung.

3. Nach der Bearbeitung der Einstellungen, klicken Sie auf **OK**, um die ausgeführten Änderungen zu speichern, oder auf **Abbrechen**, um sie aufzugeben.



In allen Dialogfenstern können Sie auf F1 klicken, um Informationen über das aktive Fenster zu erhalten. Um Kontexthilfe über einen Fensterbereich zu erhalten, klicken Sie mit der rechten Maustaste darauf.

9.2.1. Scan-Einstellungen



Die Einstellungen des Standardprogramms sind für die meisten Anwendungen optimal und sind ohne Not nicht zu verändern.

Um SpIDer Guard Dateimonitor einzustellen:

1. Wählen Sie den Menüpunkt **SpIDer Guard Einstellungen** → **Scaneinstellungen** im Kontextmenü des **Agenten** aus.



Der Menüpunkt **SpIDer Guard Einstellungen** ist im Kontextmenü des **Agenten** nur zugänglich, wenn der Benutzer:

1. Rechte, die diese Einstellungen ändern lassen, besitzt. Die Rechte werden vom Administrator des Antivirus-Netzwerkes auf dem **Server** festgesetzt.
2. Administratorrechte auf diesem Computer besitzt.

2. Es öffnet sich das Einstellungsfenster mit folgenden Abschnitten:
   - Abschnitt Scanoptionen, in dem der Prüfungsmodus der Dateien und Prozesse des geschützten Computers konfiguriert wird.

- Abschnitt Dateitypen, in dem es bestimmt wird, welche Dateien durch den Wächter zu den im Tab Prüfung festgesetzten Bedingungen zu prüfen sind.
- Abschnitt Aktionen, in dem die Reaktion des **SpIDer Guard** Wächters auf Entdeckung infizierter oder verdächtiger Dateien sowie Malware konfiguriert wird.
- Abschnitt Logdatei, in dem der Modus der Protokolldateiführung des **SpIDer Guard** Wächters konfiguriert wird.
- Abschnitt Ausschlüsse, in dem eine Liste der Ordner und Dateien, die vom Scannen durch den **SpIDer Guard** Wächter ausgeschlossen werden, konfiguriert wird.

3. Nehmen Sie die erforderlichen Änderungen vor.
4. Nach der Bearbeitung der Einstellungen, klicken Sie auf **OK**, um die ausgeführten Änderungen zu speichern, oder auf **Abbrechen**, um sie aufzugeben.

9.2.1.1. Scanoptionen

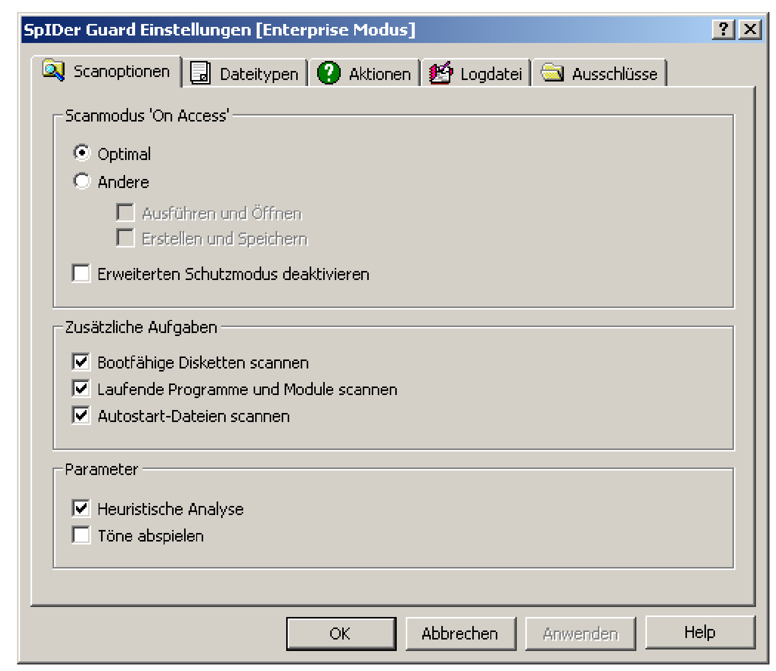


Abbildung 9-5. Einstellungsfenster von SpIDer Guard. Tab Scanoptionen.

Um Info über die Parameter in einem anderen Tab zu erhalten, klicken Sie auf entsprechenden Tabnamen in der Abbildung

Im Tab **Scanoptionen** wird der Prüfungsmodus der Dateien und Prozesse des geschützten Compuetrs konfiguriert.

Scanmodus "On Access"

Im Abschnitt **Scanmodus "On Access"** wird der Prüfungsmodus geregelt, in dem es festgesetzt wird, bei welchen Aktionen ein Objekt vom **SpIDer Guard** Wächter geprüft werden soll:



- Wird ein Häkchen bei **Optimal** gesetzt, so werden die Dateien und Bootsektoren auf Festplatten nur bei manchen Zugriffen darauf gescannt: wenn sie für Ausführung gestartet werden, beim Erstellen, beim Schreiben (beim Versuch zu schreiben) in die bestehenden Dateien und Bootsektoren.

  Die Objekte auf Wechseldatenträgern und Netzwerklaufwerken werden bei beliebigem Zugriff darauf gescannt: wenn sie für Ausführung gestartet werden, beim Erstellen, beim Schreiben (beim Versuch zu schreiben) in die bestehenden Dateien sowie beim beliebigen Öffnen der Dateien, einschließlich der Dateien nur zum Lesen.

- Wird die Variante **Andere** ausgewählt, werden folgende Modi dabei zugänglich sein:
  - **Ausführen und Öffnen** - regelt die Prüfung sämtlicher Dateien beim Ausführen sowie beim beliebigen Öffnen der Dateien, eingeschlossen von Dateien nur zum Lesen.
  - **Erstellen und Speichern** - regelt die Prüfung sämtlicher Dateien beim Erstellen oder Schreiben (beim Versuch zu schreiben) in die bestehende Dateien oder Bootsektoren.

  Mit Hilfe dieser Häkchen können Sie das Sicherheitsniveau Ihres Computers selbstständig definieren.



Beim gleichzeitigen Setzen der Häkchen bei **Ausführen und Öffnen** und **Erstellen und Speichern** wird der maximale Schutz sichergestellt, dabei aber wird die Belastung des Computers wesentlich steigen.

Präzisierungen und Empfehlungen

Es wird empfohlen, den **Optimal** Modus nur nach einer sorgfältigen Prüfung aller Festplatten unter Anwendung von **Dr.Web Scanner** zu nutzen. Dabei wird das Eindringen neuer Viren und anderer schädlichen Programme auf den Computer über die Wechseldatenträger verhindert. Es wird jedoch hierbei kein wiederholtes Scannen der bereits geprüften, "sauberen" Objekte durchgeführt.



Die Reaktion des **SpIDer Guard** Wächters auf die Entdeckung schädlicher Objekte wird im Abschnitt Aktionen konfiguriert.



Manche externe Speicher (insbesondere externe Festplatten mit USB-Schnittstelle) können im Betriebsystem als Festplatten angezeigt werden. Deswegen sollen solche Geräte unter besonderer Vorsicht genutzt und beim Anschließen an Computer auf Viren unter Anwendung von **Dr.Web Scanner** geprüft werden.

- Das Häkchen **Erweiterten Schutzmodus deaktivieren** lässt diesen Modus deaktivieren. Standardmäßig wird der erweiterte Schutzmodus eingeschaltet. In diesem Modus prüft der Wächter sofort alle Dateien, die einstellungsgemäß geprüft werden sollen. Übrige Dateien, die geöffnet werden sollen, werden in eine Warteschlange zur späteren Prüfung gestellt (Dateien, die sich zum Lesen in dem **Optimal** und im Modus **Erstellen und Speichern** öffnen). Bei geringer CPU-Auslastung werden diese Dateien auch vom Wächter geprüft.

Zusätzliche Aufgaben

- das Häkchen bei **Bootfähige Disketten scannen** lässt prüfen, ob Diskette im Diskettenlaufwerk ist. Falls die Diskette im Diskettenlaufwerk entdeckt wird, wird sie auf Viren geprüft (ist die Diskette infiziert, kann der Computer beim nächsten Herunterladen auch infiziert werden).
- das Häkchen bei **Laufende Programme und Module scannen** lässt die Dateien der Programme prüfen, die zu diesem Zeitpunkt aktiv sind.
- das Häkchen bei **Autostart-Dateien scannen** lässt sämtliche Autorun-Dateien prüfen (im `Autorun` Ordner, `ini`-Systemdateien, Windows Registrierdatenbank).



Parameter

- Setzen Sie ein Häkchen bei **Heuristische Analyse**, um diese bei Prüfung zu verwenden.

  Entfernen Sie das Häkchen, um die Prüfung nur aufgrund der bekannten Virensignaturen auszuführen (s. auch Abschnitt Entdeckungsverfahren von Viren).

- Das Häkchen **Töne abspielen** regelt die Nutzung von akustischen Reaktionen des Wächters. Standardgemäß sind die Töne abgeschaltet.

9.2.1.2. Dateitypen

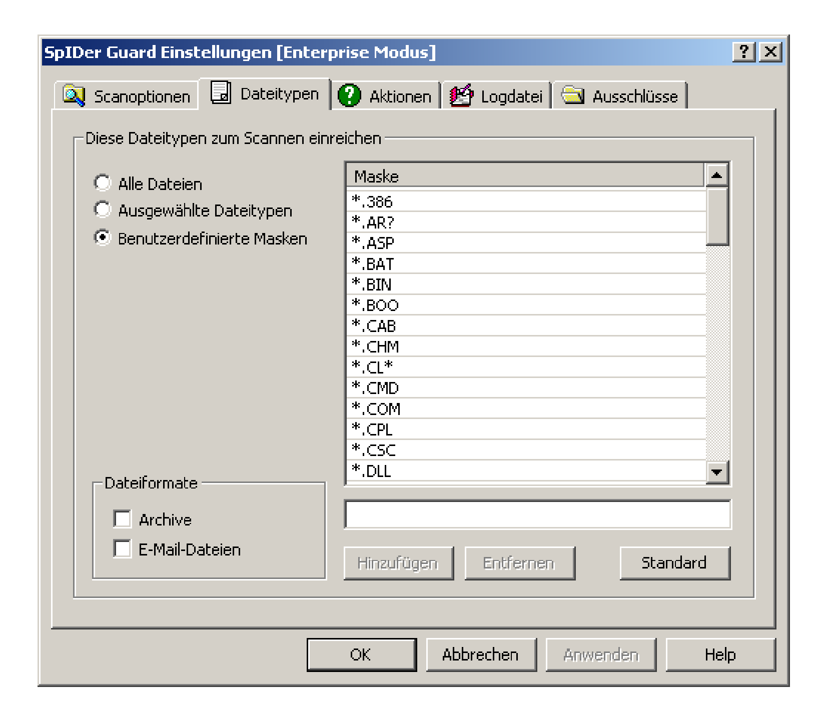


Abbildung 9-6. Einstellungsfenster von SpIDer Guard. Tab Dateitypen.

Um Info über die Parameter in einem anderen Tab zu erhalten, klicken Sie auf entsprechenden Tabnamen in der Abbildung

Im Tab **Dateitypen** wird die zusätzliche Einschränkung für Dateien festgesetzt, die gemäß den im Tab Prüfung angeführten Bedingungen zu prüfen sind.

Im Abschnitt **Diese Dateitypen zum Scannen einreichen** wählen Sie aus, welche Dateitypen vom Wächter geprüft werden sollen:

- Standardgemäß wird die Option **Alle Dateien** ausgewählt. Dabei sind alle Dateien gemäß den im Tab Prüfung angeführten Bedingungen zu prüfen. Diese Variante gewährt den maximalen Schutz.
- Die Optionen **Ausgewählte Dateitypen** und **Benutzerdefinierte Masken** schreiben vor, die Dateien zu überprüfen, deren Erweiterungen oder Namen zur Liste gehören, die sich im rechten Tabbereich befindet. Diese Liste wird beim Setzen eines dieser Häkchen aktiv.

  Standardmäßig enthält die Liste die Erweiterungen grundsetzender Dateitypen, die ein Virus enthalten können, sowie die Erweiterungen grundsetzender Archivtypen. Sie können diese Liste bearbeiten.

Die Liste der zu prüfenden Dateien erstellen

1. Um die Liste der zu prüfenden Dateien zu erstellen, führen Sie eine der Aktionen aus:
   - um die Liste von Erweiterungen der zu prüfenden Dateien zu erstellen, setzen Sie ein Häkchen bei **Ausgewählte Dateitypen** und geben Sie die Dateierweiterung im Eingabefeld unter der Liste an;
   - um die zu prüfenden Dateien festzusetzen, setzen Sie ein Häkchen bei **Benutzerdefinierte Masken** und geben Sie die Maske, die diese Dateien definiert, im Eingabefeld unter der Liste an.

   ▸ Mehr zu Masken

   Eine Maske setzt das Template für die Definition des Objektes fest. Sie kann sowohl übliche Zeichen, die für Dateinamen erlaubt sind, als auch spezielle Bezeichnungen beinhalten:

   - `*` ersetzt eine beliebige (darunter auch leere) Folge beliebiger Zeichen;
   - `?` ersetzt ein beliebiges Zeichen in bestimmter Position.

   Beispiele:

   - **bericht*.doc** – Maske, die alle Dokumente von Microsoft Word definiert, deren Name mit der bericht-Zeichenfolge anfängt, z.B. die Dateien `bericht-februar.doc`, `bericht121209.doc` usw.;



- ***.exe** – Maske, die alle ausführbaren Dateien mit der EXE Erweiterung definiert, z.B. setup.exe, iTunes.exe usw.;
- **photo????09.jpg** – Maske, die alle Dateien von JPG Bildern definiert, deren Name mit der photo Zeichenfolge anfängt und mit der Zeichenfolge `09` endet, wobei der Dateiname vier beliebige Zeichen zwischen den angegebenen Zeichenfolgen enthält, z.B. `photo121209.jpg`, `photomama09.jpg` oder `photo----09.jpg`.

2. Klicken Sie auf **Hinzufügen**.
3. Bei Bedarf wiederholen Sie die Schritte 1 und 2, um andere Typen oder Masken der Dateien hinzuzufügen.
4. Um ein Element aus der Liste der zu prüfenden Dateien zu entfernen, wählen Sie dieses Element in der Liste aus und klicken Sie auf **Entfernen**.
5. Um die standardmäßige Liste auszuwählen, klicken Sie auf den **Basis**-Knopf.

In diesem Tab wird auch der Prüfungsmodus für Dateiarchive und E-Mail-Dateien im Abschnitt **Dateiformate** festgesetzt:

- Setzen Sie ein Häkchen bei **Archive**, um verpackte Dateien zu prüfen. Standardmäßig werden die Dateien in Archiven nicht geprüft, wenn auch der Typ oder die Maske der Datei, die dem Archiv entsprechen, in der Liste der zu prüfenden Dateitypen oder –masken angegeben sind (falls eine Datei im Archiv infiziert ist, wird der Virus vom Wächter bei Verpackung entdeckt, bevor der Computer infiziert wird).



Beim Aktivieren dieser Prüfung wird die Belastung des Computers wesentlich steigen.

- Setzen Sie ein Häkchen bei **E-Mail-Dateien**, um diese Dateien zu prüfen. Die Postfächer werden vordefiniert nicht geprüft (wenn eine Datei im Anhang infiziert ist, wird ders Virus vom Wächter entdeckt, bevor der Computer infiziert wird).





Das Aktivieren dieser Option erhöht wesentlich die CPU-Auslastung.

Für den proaktiven Schutz gegen Viren in E-Mails verwenden Sie den **SpIDer Mail** E-Mail-Wächter.

9.2.1.3. Aktionen

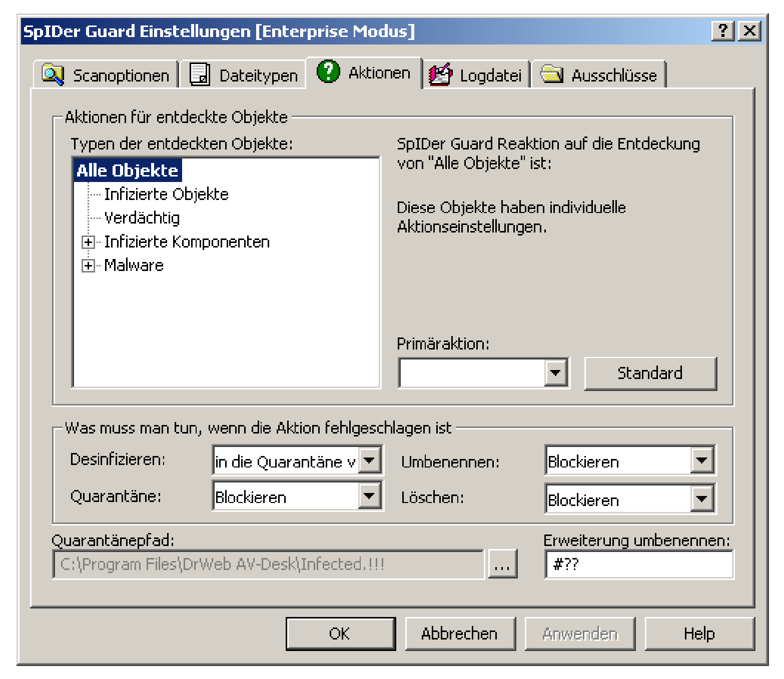


Abbildung 9-7. Einstellungsfenster von SpIDer Guard. Tab Aktionen. Um Info über die Parameter in einem anderen Tab zu erhalten, klicken Sie auf entsprechenden Tabnamen in der Abbildung

Im Tab **Aktionen** wird die Reaktion des **SpIDer Guard** Wächters bei Entdeckung infizierter oder verdächtiger Dateien und Schadprogramme konfiguriert. Die zugänglichen Reaktionen unterscheiden sich je nach dem Typ des Virenereignisses.



Aktionen einstellen

Alle Typen der schädlichen Objekte sind in der hierarchischen Liste im linken Fensterbereich dargestellt. Bei der Auswahl eines Objektes aus der Liste wird die standardmäßige Reaktion der Software auf seine Entdeckung im rechten Bereich des Fensters widerspiegelt. Es wird die Aktion angegeben, die von den gültigen Einstellungen vorgeschrieben wird, sowie die Aktionsfolge im Falle, wenn diese misslingt.

Sie haben die Möglichkeit, die Reaktionen der Software auf Entdeckung jedes Typs der Objekte separat zu verändern.

Zur Festsetzung der Aktionen für entdeckte schädliche Objekte werden folgende Einstellungen verwendet:

1. Um die Einstellungen der ersten Aktion zu ändern, geben Sie in der ausfallenden Liste **Primäraktion** die primäre Programmreaktion ein.
2. Im Bereich **Was muss man tun, wenn die Aktion fehlgeschlagen ist** werden die Aktionen bestimmt, die beim Fehlschlagen folgender Grundaktionen ausgeführt werden: Wiederherstellen, in **Quarantäne** verschieben, Umbenennen, Löschen.

Mögliche Aktionen

Folgende Aktionen können für gefundene Objekte ausgeführt werden:

- **Desinfizieren** – den Zustand des infizierten Objektes vor seiner Infizierung wiederherstellen.

  Diese Aktion ist nur für die mit bekannten desinfizierbaren Viren infizierten Objekte möglich. Ausgenommen sind Trojaner und infizierte Dateien innerhalb der zusammengesetzten Objekte (Archive, E-Mail-Dateien oder Datei-Container).

- **Löschen** – infizierte oder verdächtige Objekte löschen (für Bootsektoren werden keine Aktionen ausgeführt).





Standardmäßig überprüft die Software keine Dateiarchive sowie lässt sie nicht löschen. Ist die Prüfung von Dateiarchiven eingeschaltet (das Einschalten dieser Prüfung lässt die Belastung des Computers erheblich steigern), so können Sie die Auswahl der Aktion **Löschen** für Archiv freigeben. Dazu öffnen Sie die Konfigurationsdatei des Programms (die `drweb32.ini` Datei im Installationsordner der Software) im Texteditor und fügen Sie die Zeile `EnableDeleteArchiveAction=Yes` (oder, wenn diese Zeile vorhanden ist, ersetzen Sie den Wert `No` mit `Yes`) im Abschnitt `[SpIDerGuardNT]` hinzu. Speichern Sie die Datei.

Für die Dateien innerhalb von Archiven sind keine Aktionen möglich. Bei der Auswahl der Aktion **Löschen** wird das Archiv komplett gelöscht.

- **In die Quarantäne verschieben** – infizierte Objekte in den Quarantäne-Ordner verschieben, der im Feld **Quarantäne-Ordner** festgelegt wird (standardmäßig ist es der `infected.!!!` Unterordner im Installationsordner des Programms).
- **Benachrichtigen** – nur eine Benachrichtigung bei Virenfund senden (im Fenster Anfrage an Benutzer).
- **Blockieren** – schreibt vor, den Zugriff auf die Datei zu verweigern, deren Überprüfung die Reaktion des Wächters hervorgerufen hat. Das Sperren des Zugriffs auf die Datei wird nach dem Neustarten des Computers, sowie beim zeitweisen Deaktivieren vom Monitoring aufgehoben.
- **Ignorieren** – das Objekt ohne Anwendung jeglicher Aktionen und ohne Benachrichtigung überspringen.



Wird die Aktion **Ignorieren** ausgewählt, werden keine Aktionen ausgeführt: im Gegensatz zur aktivierten Option **Benachrichtigen** erhält der Benutzer keine Benachrichtigung bei Entdeckung eines schädlichen Objektes.



- **Umbenennen** schreibt vor, die Namenserweiterung des infizierten oder verdächtigen Objektes entsprechend der Maske, die im Feld **Maske zur Umbenennung** angegeben ist (standardmäßig `#??`, d. h. das erste Erweiterungszeichen mit `#` zu ersetzen), umzubenennen.

Tabelle 4. SpIDer Guard Aktionen bei entdeckten schädlichen Objekten

Aktion	Objekt	
	Infizierte Objekte	Verdächtig
Desinfizieren	+/*	
Löschen	+	+
In Quarantäne verschieben	+	+/*
Benachrichtigen	+	+
Blockieren	+	+
Ignorieren		+
Umbenennen	+	+

Tabelle 5. SpIDer Guard Aktionen für zusammengesetzte Objekte

Aktion	Zusammengesetztes Objekt		
	Archive	E-Mails	Container
In Quarantäne verschieben	+/*	+	+/*
Benachrichtigen	+	+/*	+
Blockieren	+	+	+
Ignorieren	+	+	+
Umbenennen	+	+	+



Tabelle 6. SpIDer Guard Aktionen für Malware

Aktion	Schädliches Objekt				
	Adware	Dialer	Scherzprogramme	Riskware	Hacktools
Löschen	+	+	+	+	+
In Quarantäne verschieben	+	+	+	+	+
Benachrichtigen	+/*	+/*	+/*	+	+/*
Blockieren	+	+	+	+	+
Ignorieren	+	+	+	+/*	+
Umbenennen	+	+	+	+	+

Symbole

+	Die Aktion ist für diesen Typ der Objekte freigegeben
+/*	Die Aktion ist als standardmäßige Reaktion für diesen Typ der Objekte festgesetzt



Bei Entdeckung der Objekte, die **Adware** oder **Dialer** enthalten, wird der Wächter im Umfang des **Dr.Web für Server** Pakets standardmäßig die Aktion **In die Quarantäne verschieben** ausführen, der Wächter im **Dr. Web für Workstations** Paket – die Aktion **Benachrichtigen**.

Reaktion bei Entdeckung

Bei Entdeckung eines infizierten oder verdächtigen Objektes sind folgende Reaktionen je nach Version des Wächters möglich:

- **SpIDer Guard** im **Dr.Web für Workstations** Paket fordert standardmäßig die Aktion des Benutzers an. Dabei wird das Fenster Anfrage an Benutzer angezeigt, in dem Sie im weiteren benötigte Aktionen für Programm manuell festsetzen können.



- **SpIDer Guard** im **Dr.Web für Server** Paket führt standardmäßig automatische Aktionen zur Vorbeugung der Virenbedrohung aus.

9.2.1.4. Logdatei

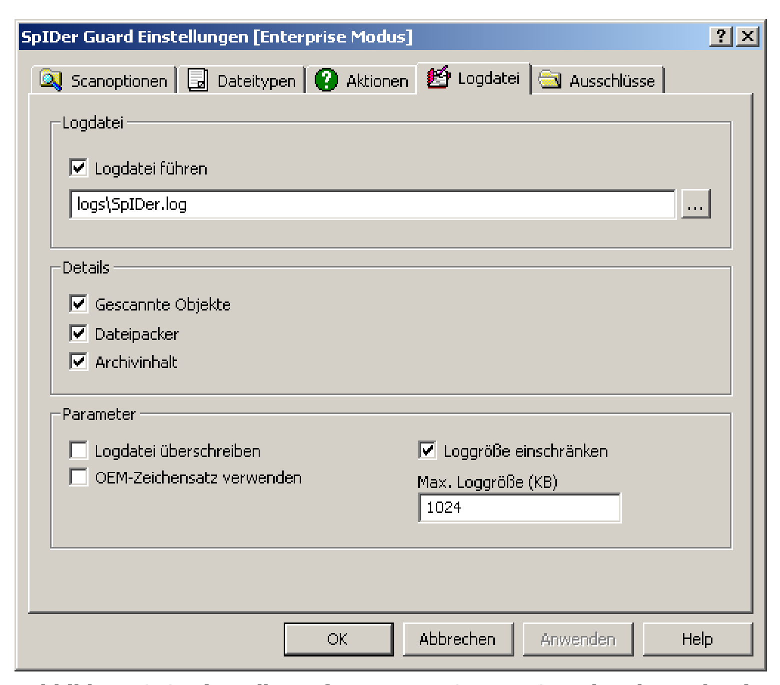


Abbildung 9-8. Einstellungsfenster von SpIDer Guard. Tab Logdatei. Um Info über die Parameter in einem anderen Tab zu erhalten, klicken Sie auf entsprechenden Tabnamen in der Abbildung

Im Tab **Logdatei** wird der Modus der Protokollführung festgesetzt und Information angegeben, die in die Protokolldatei eingetragen wird.



Es empfiehlt sich, die Protokolldatei zu führen und sie regelmäßig zu analysieren.

Protokoll

Im Abschnitt **Logdatei** werden die allgemeinen Parameter der Protokolldatei festgesetzt.

Setzen Sie ein Häkchen bei **Logdatei führen**, um die Angaben über Funktion des **SpIDer Guard** Wächters in die Protokolldatei einzutragen.

Sie können auch den Namen und den Pfad der Protokolldatei im entsprechenden Feld eingeben. Standardmäßig wird das Protokoll des **SpIDer Guard** Wächters in `logs/SpIDer.log` geschrieben, die sich im Installationsordner von **Dr.Web Enterprise Security Suite** befindet.

Details

Im Abschnitt **Details** wird die zusätzliche Information, die ins Protokoll eingetragen wird, angegeben.

Zur Detaillierung des Protokolls können folgende Häkchen gesetzt werden:

- **Gescannte Objekte** - regelt die Eintragung der Namen von allen geprüften Objekten, eingeschlossen von nicht infizierten Objekten mit dem `Ok` Vermerk (in diesem Modus kann die Protokolldatei wesentlich größer werden). Standardmäßig wird dieses Häkchen nicht gesetzt.
- **Dateipacker** - regelt die Eintragung der Meldungen über die Entdeckung von ausführbaren Dateien, die mit speziellen Packprogrammen verpackt wurden, sowie der Namen dieser Packprogramme.
- **Archivinhalt** - regelt die Eintragung der Meldungen über geprüfte Archive und über Programme, mit denen diese Archive erstellt wurden, sowie über die damit verbundenen Fehler (z.B. Archiv wurde nicht entpackt, da es mit Passwort geschützt ist).



Parameter

Im Abschnitt **Parameter** werden die zusätzlichen Parameter für Führung der Protokolldatei festgesetzt:

- Setzen Sie ein Häkchen bei **Logdatei überschreiben**, um alte Protokolldatei zu löschen und eine neue Protokolldatei am Anfang jeder neuer Sitzung zu führen. Wird dieses Häkchen entfernt, so werden die Protokolldaten am Ende der bestehenden Datei geschrieben.
- Setzen Sie ein Häkchen bei **OEM-Zeichensatz verwenden**, um die Protokolldatei in DOS-Codierung zu führen.
- Wenn Sie die Größe der Protokolldatei einschränken möchten, setzen Sie ein Häkchen bei **Loggröße einschränken** und geben Sie die maximal zulässige Dateigröße in KB im Feld **Max. Loggröße (KB)** an. Wird die maximal zulässige Größe überstiegen, so wird die Protokolldatei bereinigt und die Information wird vom Anfang an eingetragen.



9.2.1.5. Ausschlüsse

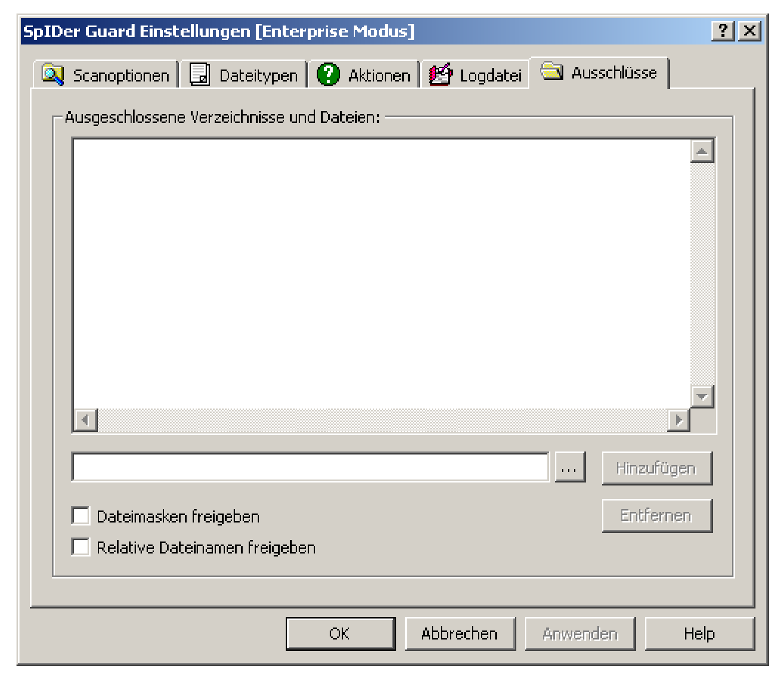


Abbildung 9-9. Einstellungsfenster von SpIDer Guard. Tab Ausschlüsse.

Um Info über die Parameter in einem anderen Tab zu erhalten, klicken Sie auf entsprechenden Tabnamen in der Abbildung

Im Tab **Ausschlüsse** wird die Liste der Ordner und Dateien, die vom Prüfungsvorgang durch den **SpIDer Guard** Wächter ausgenommen werden.

Im Abschnitt **Ausgeschlossene Verzeichnisse und Dateien** wird eine Auflistung von Ordnern und Dateien zusammengestellt, welche von der Prüfung mit dem **SpIDer Guard** Wächter ausgeschlossen sind. Dies können die Quarantäne-Ordner des Antivirus, Arbeitsordner mancher Programme, temporäre Dateien (Swap-Dateien) u.ä. sein.



Standardmäßig ist die Liste leer. Sie können sowohl bestimmte Ordner und Dateien zu den Ausnahmen hinzufügen, als auch Masken verwenden, um die Prüfung von bestimmten Objektgruppen zu verbieten.

Ausnahmenliste erstellen

1. Um einen Ordner oder eine Datei zur Ausnahmenliste hinzuzufügen, führen Sie eine der folgenden Aktionen aus:
   - um einen bestimmten bestehenden Ordner oder eine Datei anzugeben, klicken Sie auf den <**...**> Knopf und wählen Sie einen Ordner oder eine Datei im standardmäßigen Betriebssystem-Browser aus. Außerdem können Sie den kompletten Pfad der Datei oder des Ordners manuell im Eingabefeld angeben;
   - um alle Dateien oder Ordner mit einem bestimmten Namen von der Prüfung auszunehmen, ohne dabei den bestimmten Pfad anzugeben, setzen Sie ein Häkchen bei **Relative Dateinamen freigeben** freigen. Danach geben Sie den erforderlichen Namen in das Eingabefeld ein;
   - um die Dateien oder Ordner einer bestimmten Art von der Prüfung auszunehmen, setzen Sie ein Häkchen bei **Dateimasken freigeben**. Danach geben Sie eine Maske in das Eingabefeld ein.

   Mehr zu Masken

   Eine Maske setzt das Template für die Definition des Objektes fest. Sie kann sowohl übliche Zeichen, die für Dateinamen erlaubt sind, als auch spezielle Bezeichnungen beinhalten:

   - `*` ersetzt eine beliebige (darunter auch leere) Folge beliebiger Zeichen;
   - `?` ersetzt ein beliebiges Zeichen in bestimmter Position.

   Beispiele:

   - **bericht*.doc** – Maske, die alle Dokumente von Microsoft Word definiert, deren Name mit der bericht-Zeichenfolge anfängt, z.B. die Dateien `bericht-februar.doc`, `bericht121209.doc` usw.;



- ***.exe** – Maske, die alle ausführbaren Dateien mit der EXE Erweiterung definiert, z.B. setup.exe, iTunes.exe usw.;
- **photo????09.jpg** – Maske, die alle Dateien von JPG Bildern definiert, deren Name mit der photo Zeichenfolge anfängt und mit der Zeichenfolge `09` endet, wobei der Dateiname vier beliebige Zeichen zwischen den angegebenen Zeichenfolgen enthält, z.B. `photo121209.jpg`, `photomama09.jpg` oder `photo----09.jpg`.

2. Klicken Sie auf **Hinzufügen**.
3. Bei Bedarf wiederholen Sie die Schritte 1 und 2, um andere Dateien oder Ordner hinzuzufügen.
4. Um eine Datei oder einen Ordner aus der Liste der Ausnahmen zu entfernen, wählen Sie das entsprechende Element in der Liste aus und klicken Sie auf **Entfernen**.

9.2.2. Verwaltung



Die Einstellungen des Standardprogramms sind für die meisten Anwendungen optimal und sind ohne Not nicht zu verändern.

Um SpIDer Guard Dateimonitor einzustellen:

1. Im Kontextmenü des **Agenten** wählen Sie den Menüpunkt **SpIDer Guard Einstellungen** → **Verwaltung** aus oder wählen Sie das **SpIDer Guard** Element, das sich in der Windows **Systemsteuerung** befindet, aus.



Der Menüpunkt **SpIDer Guard Einstellungen** ist im Kontextmenü des **Agenten** nur zugänglich, wenn der Benutzer:

1. Rechte, die diese Einstellungen ändern lassen, besitzt. Die Rechte werden vom Administrator des Antivirus-Netzwerkes auf dem **Server** festgesetzt.
2. Administratorrechte auf diesem Computer besitzt.



2. Es öffnet sich das Einstellungsfenster mit folgenden Abschnitten:
   - Verwaltung;
   - Parameter;
   - Notifizierung;
   - Reminder.
3. Nehmen Sie die erforderlichen Änderungen vor.
4. Nach der Bearbeitung der Einstellungen, klicken Sie auf **OK**, um die ausgeführten Änderungen zu speichern, oder auf **Abbrechen**, um sie aufzugeben.



9.2.2.1. Verwaltung

SpIDer Guard [Enterprise Modus]

Verwaltung | Parameter | Notifizierung | Reminder

SpIDer Guard für Windows
(c) Doctor Web, Ltd., 1992-2010

Status
SpIDer Guard schützt Ihr System

Lademodus
Manuell
Automatisch
Installationspfad:
C:\Program Files\DrWeb AV-Desk

Beenden
Deinstallieren

Enterprise Modus: Online

OK | Abbrechen | Anwenden | Help

Abbildung 9-10. Einstellungsfenster von SpIDer Guard. Tab Verwaltung.

Um Info über die Parameter in einem anderen Tab zu erhalten, klicken Sie auf entsprechenden Tabnamen in der Abbildung

Im Tab **Verwaltung** wird der Lademodus von **SpIDer Guard** festgesetzt sowie die Registrierung der Komponente im Betriebssystem ausgeführt (oder abgestellt).



Der Abschnitt **Lademodus** lässt die Variante des Programmstartes auswählen:

- Falls **Manuell** ausgewählt wird, klicken Sie auf **Starten**, um den Wächter zu starten. Der auf solche Weise gestartete Wächter kann mit dem Klicken auf **Beenden** gestoppt werden.
- Falls **Automatisch** ausgewählt wird, wird der Wächter beim jeden Herunterladen von Windows automatisch gestartet.

Um den Wächter im Betriebssystem zu registrieren, klicken Sie auf **Installieren**. Um die Registrierung abzustellen, klicken Sie auf **Deinstallieren**.

Nach Installation von **Antivirus** wird der Wächter standardmäßig automatisch bei jedem Start des Betriebssystems aktiviert. Sie können aber den Lademodus von **SpIDer Guard** ändern, wobei Sie den automatischen Modus deaktivieren.

Um das automatische Starten von SplDer Guard zu deaktivieren:

1. Gehen Sie zum Tab Verwaltung im entsprechenden Fenster von **SpIDer Guard** über.



Der Menüpunkt **SpIDer Guard Einstellungen** → **Verwaltung** ist im Kontextmenü des **Agenten** nur zugänglich, wenn der Benutzer:

1. Rechte, die diese Einstellungen ändern lassen, besitzt. Die Rechte werden vom Administrator des Antivirus-Netzwerkes auf dem **Server** festgesetzt.
2. Administratorrechte auf diesem Computer besitzt.

2. Im Fensterbereich **Lademodus** wählen Sie **Manuell** aus.
3. Klicken Sie auf **OK**.

   Beim nächsten Starten von Windows wird das Programm automatisch nicht gestartet. Bei Bedarf können Sie es manuell starten. Dafür klicken Sie auf **Starten** im oben genannten Fensterbereich. Der manuell gestartete Wächter kann mit dem Klicken auf **Beenden** gestoppt werden.

9.2.2.2. Parameter

SpIDer Guard [Enterprise Modus]

Verwaltung | Parameter | Notifizierung | Reminder

Leistungsfähigkeit

Maximalgröße der Liste der gescannten Dateien: 1000

Deaktiviert | Maximal

Die Liste der gescannten Dateien soll ungefähr 97 KB groß sein

Sonstiges

- [ ] SpIDer Guard Icon im Infobereich anzeigen
- [ ] 'Monitoring anhalten' zwischen Sitzungen speichern

Spezielle Einstellungen

- [x] Objekte im Lokalnetzwerk nicht scannen
- [ ] Objekte auf Wechseldatenträgern nicht scannen

OK | Abbrechen | Anwenden | Help

Abbildung 9-11. Einstellungsfenster von SpIDer Guard. Tab Parameter.

Um Info über die Parameter in einem anderen Tab zu erhalten, klicken Sie auf entsprechenden Tabnamen in der Abbildung

In diesem Tab von **SpIDer Guard** werden einzelne Einstellungen des Wächters festgesetzt.



Leistungsfähigkeit

Im Abschnitt **Leistungsfähigkeit** wird die Größe der Pfadliste von geprüften Dateien, die im Cache-Speicher gespeichert wird, festgesetzt.

Bewegen Sie den Schieberegler, um die Größe dieser Lsite zu bestimmen.

Die Dateien aus dieser Liste werden von wiederholten Prüfungen ausgenommen, wenn sie nicht geändert wurden. Standardmäßig beträgt dieser Parameterwert 100, d.h. 9 KB vom benutzten Speicher für jeden logischen Datenträger. Wenn das Betriebssystem genügend Speicherplatz hat, so kann dieser Parameterwert bis zu 500-1000 vergrößert werden. Dieser Parameter ist nur im Prüfungsmodus **Ausführen und Öffnen** sowie bei Prüfung der Dateien auf Netzwerklaufwerken und Wechseldatenträgern im **Optmal** aktuell.

Sonstiges

Im Abschnitt **Sonstiges** können Sie folgende Einstellungen festsetzen:

- Setzen Sie ein Häkchen bei **SpIDer Guard Icon im Infobereich anzeigen**, wenn Sie möchten, dass das Wächter-Icon im Infobereich der Taskleiste (Element von Microsoft Windows Desktop, das Icons aktiver Anwendungen anzeigt und sich im rechten Bereich der Taskleiste befindet. Die Taskleiste befindet sich standardmäßig im unteren Bereich des Desktops) von Windows angezeigt wird.
- Beim Setzen eines Häkchens bei **'Monitoring anhalten' zwischen Sitzungen speichern** wird der **SpIDer Guard** Wächter im Pausemodus nach Neustart bleiben, wenn Monitoring in der laufenden Sitzung abgeschaltet wurde.



Spezielle Einstellungen

Im Abschnitt **Spezielle Einstellungen** können Sie folgende Einstellungen festsetzen:

- Setzen Sie ein Häkchen bei **Objekte auf Wechseldatenträgern nicht scannen**, damit die Dateien auf Wechseldatenträgern nur beim Starten ihrer Ausführung gescannt werden.

  Wird das Häkchen bei **Objekte auf Wechseldatenträgern nicht scannen** entfernt, so werden die Dateien auf Wechseldatenträgern (CD/DVD, Magnetplatten (FDD), flash-Speicher und sonstige Datenträger, die über einen USB-Port angeschlossen werden) bei beliebigem Zugriff darauf, eingeschlossen vom Öffnen der Dateien nur zum Lesen, gescannt.

- Setzen Sie ein Häkchen bei **Objekte im Lokalnetzwerk nicht scannen**, damit die Dateien auf Netzwerklaufwerken nur beim Starten ihrer Ausführung auf Ihrem Computer gescannt werden.

  Wird das Häkchen bei **Objekte im Lokalnetzwerk nicht scannen** entfernt, so werden die Objekte auf Netzwerklaufwerken beim Starten ihrer Ausführung auf Ihrem Computer sowie beim beliebigen Öffnen der Dateien, eingeschlossen von Dateien nur zum Lesen, geprüft.



Manche externe Speicher (insbesondere externe Festplatten mit USB-Schnittstelle) können im Betriebssystem als Festplatten angezeigt werden. Deswegen sollen solche Geräte unter besonderer Vorsicht genutzt und beim Anschließen an Computer auf Viren unter Anwendung vom Antivirus-Scanner geprüft werden.



9.2.2.3. Notifizierung

Abbildung 9-12. Einstellungsfenster von SpIDer Guard. Tab Notifizierung.

Um Info über die Parameter in einem anderen Tab zu erhalten, klicken Sie auf entsprechenden Tabnamen in der Abbildung

Im Tab **Notifizierung** werden die Benachrichtigungen über entdeckte Vireneireignisse eingestellt: Liste der Ereignisse, die den Versand von Benachrichtigungen aufrufen, Versandtyp und Listen der Empfänger.



Im Abschnitt **Bei folgenden Ereignissen notifizieren** setzen Sie Häkchen bei den Typen der Ereignisse, über welche eine Benachrichtigung zu versenden ist.

Im Abschnitt **Empfänger** wird der Versandtyp von Benachrichtigungen festgesetzt:

- Setzen Sie ein Häkchen bei **Per E-Mail notifizieren**, wenn Sie Benachrichtigungen über ausgewählte Ereignisse per E-Mail senden möchten.
- Setzen Sie ein Häkchen bei **Über das Netzwerk notifizieren**, wenn Sie Benachrichtigungen über ausgewählte Ereignisse im Netzwerk senden möchten.



Die Optionen **Per E-Mail notifizieren** und **Über das Netzwerk notifizieren** sind voneinander unabhängig und können gleichzeitig ausgewählt werden.

Danach sind die Listen der Empfänger von Benachrichtigungen für ausgewählte Versandtypen zu erstellen (bearbeiten):

1. Um ein neues Element in die Liste der Empfänger von E-Mail-Benachrichtigungen hinzuzufügen, klicken Sie auf den **Hinzufügen**-Knopf bei der Liste der E-Mail-Adressen. Es öffnet sich das Einstellungsfenster der E-Mail-Adresse.
2. Um ein neues Element in die Liste der Empfänger von lokalen Netzwerk-Benachrichtigungen hinzuzufügen, klicken Sie auf den **Hinzufügen**-Knopf bei der Liste der Netzwerkadressen. Es öffnet sich das Einstellungsfenster der Netzwerkadresse.
3. Um ein Element aus der Liste zu entfernen, wählen Sie es in der entsprechenden Liste aus und klicken Sie auf **Entfernen**.
4. Um ein Element in der Liste zu bearbeiten, wählen Sie es in der Liste aus und klicken Sie auf **Bearbeiten**. Es öffnet sich das Einstellungsfenster der E-Mail-Adresse oder das Einstellungsfenster der Netzwerkadresse.



9.2.2.4. Reminder

Abbildung 9-13. Einstellungsfenster von SpIDer Guard. Tab Reminder.

Um Info über die Parameter in einem anderen Tab zu erhalten, klicken Sie auf entsprechenden Tabnamen in der Abbildung

Im Tab **Reminder** wird die Anzeige von Tipp-Erinnerungen eingestellt. Die Tipps tauchen als Popup-Meldungen über dem **SpIDer Guard** Icon im Infobereich von Windows auf, wenn die Anzeige des Wächter-Icons aktiviert ist.



Im Abschnitt **Infomeldung anzeigen, wenn** wird eine Liste von Ereignissen erstellt, über die man mit einer Popup-Meldung informiert wird:

- **Dr.Web Engine und Virendatenbanken aktualisiert sind** - über Aktualisierung von Antivirus-Engine und Virendatenbanken benachrichtigen.
- **Schaddatei desinfiziert ist** - bei Entdeckung und Desinfektion eines infizierten Objektes benachrichtigen.
- **Status geändert ist** - bei Änderungen in der Funktion des **SpIDer Guard** Wächters (Starten, Stoppen) benachrichtigen.

Das Häkchen bei **Über nicht aktualisierte Virendatenbanken benachrichtigen in** schreibt dem Wächter vor, eine Infomeldung anzuzeigen, wenn die Virendatenbanken nach Ablauf der in der ausfallenden Liste angegebenen Zeitperiode nicht aktualisiert wurden.

In der Gruppe **Reminder** wird die Anzeige von Tipps über ausgewählte Ereignisse konfiguriert:

- **Infomeldung beim Systemstart anzeigen** - Tipps bei jedem Herunterladen des Betriebssystems anzeigen.
- **Infomeldung wiederholt anzeigen in** - Wiederholte Anzeige von Erinnerungen mit den in der ausfallenden Liste ausgewählten Zeitabständen aktivieren.

Klicken Sie auf **Default-Einstellungen**, um die ursprünglichen Einstellungen, die vom Programm empfohlen werden, zu aktivieren.



9.2.3. Zusätzliche Benutzerdialoge

9.2.3.1. Anfrage an Benutzer bei Entdeckung eines infizierten Objektes

Dieses Fenster wird geöffnet, wenn ein infiziertes oder verdächtiges Objekt vom Wächter entdeckt wird, vorausgesetzt, dass die Benachrichtigungen in Programmeinstellungen festgesetzt sind.



Abbildung 9-14. Das Fenster für Anforderung der Aktionen vom Wächter bei Entdeckung eines infizierten Objektes

Die zugänglichen Knöpfe hängen vom Typ des Virenereignisses sowie vom Typ des infizierten Objektes ab (für Archive, E-Mail-Dateien und Datei-Container bleiben manche Reaktionen unzugänglich).

- Der Knopf **Ignorieren** schreibt vor, dass keine Aktionen bei Entdeckung eines verdächtigen Objektes ausgeführt werden.
- Der Knopf **Blockieren** schreibt vor, dass der Zugriff auf eine Datei, deren Prüfung die Reaktion des Wächters gebracht hat, verboten wird. Die Blockierung des Zugriffs auf die Datei wird nach dem Neustart des Computers sowie beim temporären Auschalten von Monitoring aufgehoben.
- Der Knopf **Wiederherstellen** (ist nur bei Entdeckung eines vermutlich desinfizierbaren Virus zugänglich und für Archive vom beliebigen Typ unzugänglich) schreibt vor, dass der Wächter das mit einem bekannten Virus infizierte Objekt zu desinfizieren



versucht. Wenn der Virus nicht desinfizierbar ist oder der Desinfektionsversuch fehlgeschlagen ist, wird das Fenster noch einmal in der für nicht desinfizierbare Viren festgesetzten Form angezeigt.

- Der Knopf **Umbenennen** schreibt vor, dass die Namenserweiterung einer infizierten oder verdächtigen Datei gemäß den Standardeinstellungen umbenannt wird.
- Der Knopf **Verschieben** schreibt vor, dass eine infizierte oder verdächtige Datei in den standardgemäß festgesetzten Quarantäne-Ordner verschoben wird.
- Der Knopf **Löschen** schreibt vor, dass eine infizierte oder verdächtige Datei (bei Bootsektoren werden keine Aktionen ausgeführt) gelöscht wird. Bei Standardeistellungen wird diese Reaktion für beliebige Archive unzugänglich sein.



9.2.3.2. Einstellungsfenster der E-Mail-Adresse

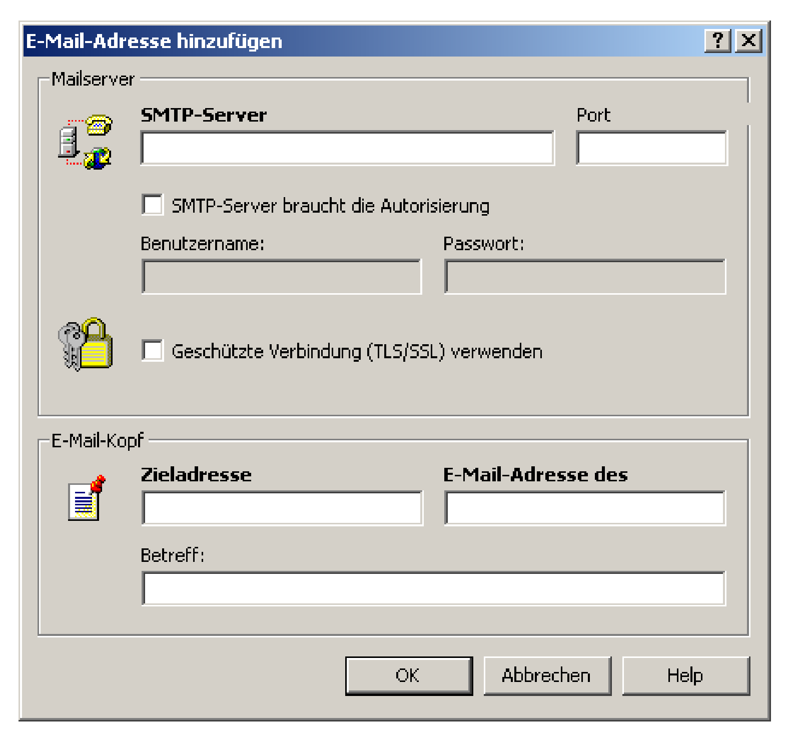


Abbildung 9-15. Einstellungsfenster der E-Mail-Adresse

In diesem Fenster werden die Adresse und die Mail-Einstellungen vom E-Mail-Postfach, das zum Empfang von Benachrichtigungen über Virenereignisse benutzt wird, festgesetzt.

Mailserver

Im Abschnitt **Mailserver** werden die Einstellungen des SMTP-Servers für E-Mail-Versand festgesetzt.



Folgende Parameter sind obligatorisch:

- **SMTP Server** - IP-Adresse oder Domainname des Servers für versandte E-Mails.
- **Port** - Nummer des Ports, auf dem SMTP-Server läuft.

Falls auf dem SMTP-Server Authorisierung benötigt wird, setzen Sie ein Häkchen bei **SMTP-Server braucht Authorisierung** und füllen Sie die Felder **Benutzername** und **Passwort** für den Zugriff auf den Server für ausgehende E-Mails aus.

Wenn es eine TLS/SSL-geschützte Verbindung benötigt wird, setzen Sie ein Häkchen bei **Geschützte Verbindung (TLS/SSL) verwenden**.

E-Mail-Kopf

Im Abschnitt **E-Mail-Header** werden die Attribute einer E-Mail festgesetzt.

Geben Sie folgende E-Mail-Adressen an:

- Im Feld **Zieladresse** geben Sie die E-Mail-Adresse an, die zum Empfang von Benachrichtigungen über Virenereignisse benutzt wird.
- Im Feld **E-Mail-adresse des** geben Sie die E-Mail-Adresse an, die als Adresse des Absenders in der Nachricht über Virensituation angezeigt wird.

Sie können auch das Thema der Nachricht im Feld **Betreff** angeben. Wenn dieses Feld nicht ausgefüllt wird, so wird der standardmäßig festgesetzte Betreff in der E-Mail angegeben.

9.2.3.3. Einstellungsfenster der Netzwerkadresse

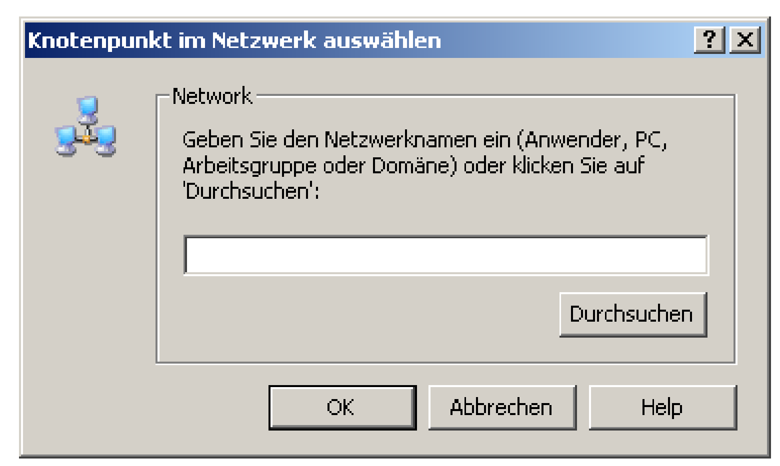


Abbildung 9-16. Einstellungsfenster der Netzwerkadresse

In diesem Fenster wird die Adresse des Computers im Microsoft Netzwerk angegeben, damit der Computer in die Benachrichtigungsliste eingetragen wird.

Geben Sie den Netzwerknamen des Computers im Feld **Computername** an oder klicken Sie auf **Durchsuchen**, um den Computer im Ordner des Netzwerk-Browsers zu finden.



Kapitel 10. SpIDer Mail

Der **SpIDer Mail** E-Mail-Wächter gehört standardgemäß zum Umfang der zu installierenden Komponenten, läuft permanent im Hauptspeicher und wird beim Starten des Betriebsystems automatisch ausgeführt.

Wenn der Antivirus unter Lizenz für das Programmpaket "Antivirus+Antispam" (und entsprechender Schlüsseldatei) funktioniert, so kann die Spam-Prüfung von E-Mails auch vom E-Mail-Wächter mit Hilfe von **Dr.Web Antispam** ausgeführt werden.

Die Standardeinstellungen von **SpIDer Mail** sind für die Anfänger optimal und sorgen für das maximale Sicherheitsniveau bei einer minimalen Einmischung seitens Benutzers. Dabei werden jedoch einige Möglichkeiten der Mail-Programme blockiert (z.B.: der Versand einer E-Mail an mehrere Adressen kann als Massenversand eingestuft werden, oder eingehende Spam-Mail wird nicht erkannt). Einige Informationen (aus dem nicht infizierten Teil des Textes) können den automatisch gelöschten Mails nicht mehr entnommen werden. Die erfahrenen Benutzer können die Parameter der E-Mail-Prüfung verändern sowie die Einstellungen für die Reaktion des **SpIDer Mail** E-Mail-Wächters auf verschiedene Ereignisse verändern.

E-mails bearbeiten

Standardgemäß werden sämtliche Zugriffe auf Mail-Server, die auf den für Protokolle standardmäßigen Ports durch beliebige Mail-Programme auf Ihrem Computer ausgeführt werden, vom **SpIDer Mail** E-Mail-Wächter automatisch abgefangen. Die Standardports sind:

- für das POP3-Protokoll - Port 110;
- für das SMTP-Protokoll - Port 25;
- für das IMAP4-Protokoll - Port 143;
- für das NNTP-Protokoll - Port 119.



In manchen Fällen ist das automatische Abfangen von POP3-, SMTP-, IMAP4- und NNTP-Verbindungen nicht möglich. In diesem Fall können Sie das Abfangen der Verbindungen per Hand einstellen.

Der **SpIDer Mail** E-Mail-Wächter empfängt alle eingehenden E-Mails anstatt des E-Mail-Clients und prüft sie auf Viren mit maximaler Detailuntersuchung. Werden keine Viren oder verdächtige Objekte gefunden, so wird die E-mail dem E-Mail-Client in einer "transparenten" Form übermittelt, als ob sie direkt vom Server kam. Auf ähnliche Weise werden die ausgehenden E-Mails vor ihrer Absendung an Server geprüft.

Dr.Web Antispam



Die Spam-Prüfung von E-Mails ist nur zugänglich, wenn **Dr. Web Agent** unter Lizenz "Antivirus+Antispam" betrieben wird.

Die Technologie des Antispamfilters von **Dr.Web** basiert auf mehreren Tausenden von Regeln, die in einige Gruppen eingeteilt werden können:

- **Heuristische Analyse** – äußerst komplizierte, hochintelligente Technologie der empirischen Auswertung aller E-Mail-Teile: des Headers, des E-Mails-Körpers, des Anhangs.
- **Filterung der Gegenwirkung** – basiert auf Erkennung von Tricks, die von Spamern zum Überspringen der Antispamfilter benutzt werden.
- **Analyse aufgrund von HTML-Signaturen** – die Nachrichten, die den HTML-Kode enthalten, werden mit den Mustern der HTML-Signaturen aus der Antispambibliothek verglichen.
- **Semantische Analyse** – Wörter und Ausdrücke in einer Nachricht werden mit den für Spam typischen Wörtern und idiomatischen Wendungen mit Hilfe eines speziellen Wörterbuches verglichen. Der Analyse werden sowohl sichtbare als auch visuell durch spezielle technische Tricks versteckte Wörter, Ausdrücke und Symbole unterzogen.
- **Anti-Scam-Technologie** – zu den Scamming- und Pharming-



Nachrichten zählen die sogenannten nigerianischen E-Mails, Nachrichten über Geldgwinn durch Lotterien, im Kasino, gefälschte Nachrichten von Banken. Für deren Filterung wird ein spezielles Modul angewendet.

- **Filterung technischer Spam-Mails** – die sogenannten Bounce-Nachrichten entstehen als Reaktion auf Viren oder als Äußerung von Virusaktivität. Das spezielle Antispam-Modul behandelt solche Nachrichten als unerwünschte.

SpIDer Mail Reaktionen

Die Reaktion des **SpIDer Mail** E-Mail-Wächters bei Entdeckung von infizierten und verdächtigen eingehenden E-Mails sowie von E-Mails, die keine Prüfung bestanden haben (z.B. E-Mails mit übermäßig komplizierter Struktur), ist standardmäßig wie folgt:

- aus den infizierten E-Mails werden schädliche Informationen entfernt (diese Aktion wird *Desinfizieren* einer E-Mail genannt), dann werden sie wie üblich zugestellt;
- E-Mails mit verdächtigen Objekten werden als einzelne Dateien in die Quarantäne verschoben, dem Mail-Programm wird eine Benachrichtigung darüber zugesandt (diese Aktion wird *Verschieben* einer E-Mail genannt);
- nicht infizierte E-Mails und E-Mails, die keine Prüfung bestanden haben, werden ohne Änderungen weitergegeben *(übersprungen);*
- alle gelöschten und verschobenen E-Mails werden auch auf dem POP3- oder IMAP4-Server gelöscht.

Infizierte oder verdächtige ausgehende E-Mails werden an Server nicht weitergeleitet. Der Benutzer wird über das fehlgeschlagene Absenden informiert (in der Regel, wird die E-Mail dabei vom Mail-Programm gespeichert).

Beim Vorhandensein eines unbekannten Virus auf dem Computer, welcher sich über E-Mail verbreitet, kann der **SpIDer Mail** E-Mail-Wächter die typischen Merkmale des "Virenverhaltens" (Massenversand) erkennen. Standardmäßig ist diese Option aktiv.



Mit dem **SpIDer Mail** E-Mail-Wächter können die eingehenden E-Mails mittels Dr.Web Antispam auf Spam geprüft werden. Standardmäßig ist diese Option aktiv.

E-Mails mit anderen Mitteln prüfen

Der **SpIDer Guard** E-Mail-Wächter sowie **Dr.Web Scanner** kann ebenfalls Viren in den E-Mail-Postfächern mancher Formate entdecken, der **SpIDer Mail** E-Mail-Wächter hat jedoch im Gegensatz dazu einige Vorteile:

- weitaus nicht alle Formate von E-Mail-Postfächern der populären Mail-Programme werden vom **SpIDer Guard** Wächter und **Dr.Web Scanner** unterstützt; mit **SpIDer Mail** E-Mail-Wächter landen infizierte E-Mails erst gar nicht in dem Postfach;
- standardmäßig prüft **SpIDer Guard** die E-Mail-Postfächer nicht; bei Aktivierung dieser Option wird die Leistungsfähigkeit des Systems wesentlich reduziert;
- **Dr.Web Scanner** prüft die E-Mail-Postfächer nur auf Anfrage des Benutzers oder gemäß dem Terminplan und nicht im Moment des E-Mail-Empfangs, dabei ist diese Aktion arbeits- und zeitaufwändig.

Somit entdeckt der **SpIDer Mail** E-Mail-Wächter unter Standardeinstellungen sämtlicher **Dr.Web Enterprise Security Suite** Komponenten als erster Viren und verdächtige Objekte, die sich über E-Mails verbreiten, und blockiert ihren Zugriff auf den Computer. Seine Funktion ist extrem ressourcensparend. Die Verwendung sonstiger Komponenten wird für die Prüfung der E-Mails nicht benötigt.

Wächter einstellen

Die Einstellungen des **SpIDer Mail** Wächters unterscheiden sich je nach installierter Version. Es sind zwei Versionen des **SpIDer Mail** Wächters vorhanden:

- SpIDer Mail,
- SpIDer Mail NT4.



Vor Installation wird die Version des Betriebssystems automatisch bestimmt und entsprechende Version des **SpIDer Mail** Wächters installiert (s. Punkt Systemanforderungen).

Gegebenenfalls (z.B. falls hinsichtlich der Prozessorbelastung kritische Aufgabe im Echtzeitmodus auszuführen ist) können Sie den Wächter temporär abschalten.

10.1. SpIDer Mail einstellen



Die Einstellungen des Standardprogramms sind für die meisten Anwendungen optimal und sind ohne Not nicht zu verändern.

Um SplDer Mail Dateimonitor einzustellen:

1. Im Kontextmenü des **Agenten** wählen Sie den Menüpunkt **SpIDer Mail Einstellungen** aus.



Der Menüpunkt **SpIDer Mail Einstellungen** ist im Kontextmenü des **Agenten** nur zugänglich, wenn der Benutzer:

1. Rechte, die diese Einstellungen ändern lassen, besitzt. Die Rechte werden vom Administrator des Antivirus-Netzwerkes auf dem **Server** festgesetzt.
2. Administratorrechte auf diesem Computer besitzt.

2. Es öffnet sich das Einstellungsfenster mit folgenden Abschnitten:
   - Abschnitt **Virenprüfung**, in dem der Prüfungsmodus für E-Mails festgesetzt wird (ausführliche Beschreibung finden Sie in der Hilfedatei **Dr.Web Antivirus für Windows**, Abschnitt **Virenprüfung**).

- Abschnitt **Antispam**, in dem der Prüfungsmodus von E-Mails auf Spam mit Hilfe von **Dr.Web Antispam** festgesetzt wird (ausführliche Beschreibung finden Sie in der Hilfedatei **Dr.Web Antivirus für Windows**, Abschnitt **Antispam**).
- Abschnitt **Ausnahmen**, in dem die Liste der Ausnahmen, deren Mail-Verkehr von der Prüfung durch **SpIDer Mail** E-Mail-Wächter ausgenommen wird (ausführliche Beschreibung finden Sie in der Hilfedatei **Dr.Web Antivirus für Windows**, Abschnitt **Ausnahmen**).
- Abschnitt **Abgefangen**, in dem die Parameter fürs Abfangen von Verbindungen zu den Mail-Servern festgesetzt werden (ausführliche Beschreibung finden Sie in der Hilfedatei **Dr.Web Antivirus für Windows**, Abschnitt **Abfangen von Verbindungen**).
- Abschnitt **Protokoll**, in dem die Führung der Protokolldatei vom **SpIDer Mail** E-Mail-Wächter eingestellt wird (ausführliche Beschreibung finden Sie in der Hilfedatei **Dr.Web Antivirus für Windows**, Abschnitt **Protokoll**).



In allen Dialogfenstern klicken Sie auf F1, um Informationen über das aktive Fenster zu erhalten.

3. Nehmen Sie die erforderlichen Änderungen vor.
4. Nach der Bearbeitung der Einstellungen, klicken Sie auf **OK**, um die ausgeführten Änderungen zu speichern, oder auf **Abbrechen**, um sie aufzugeben.

10.2. SpIDer Mail NT4 einstellen



Die Einstellungen des Standardprogramms sind für die meisten Anwendungen optimal und sind ohne Not nicht zu verändern.

Um SpIDer Mail NT4 Dateimonitor einzustellen:

1. Im Kontextmenü des **Agenten** wählen Sie den Menüpunkt **SpIDer Mail Einstellungen** aus.



Der Menüpunkt **SpIDer Mail Einstellungen** ist im Kontextmenü des **Agenten** nur zugänglich, wenn der Benutzer:

1. Rechte, die diese Einstellungen ändern lassen, besitzt. Die Rechte werden vom Administrator des Antivirus-Netzwerkes auf dem **Server** festgesetzt.
2. Administratorrechte auf diesem Computer besitzt.

2. Es öffnet sich das Einstellungsfenster mit folgenden Abschnitten:
   - Abschnitt Scan (Virenprüfung), in dem der Prüfungsmodus für E-Mails festgesetzt wird.
   - Abschnitt Actions (Aktionen), in dem die Reaktion des **SpIDer Mail** Wächters bei Entdeckung infizierter oder verdächtigen Dateien in E-Mails festgesetzt wird.
   - Abschnitt Engine, in dem die Parameter für Funktion der Antivirus-Engine festgesetzt werden.
   - Abschnitt Log (Protokoll), in dem die Führung der Protokolldatei vom **SpIDer Mail** Wächter eingestellt wird.
   - Abschnitt Interception (Abfangen), in dem die Parameter fürs Abfangen von Verbindungen zu den POP3/SMTP/IMAP4/NNTP-Servern festgesetzt werden.
   - Abschnitt Excluded Applications (Ausgenommene Anwendungen), in dem die Liste der Ordner und Dateien, die von der Prüfung durch den **SpIDer Mail** Wächter ausgenommen werden.
3. Nehmen Sie die erforderlichen Änderungen vor.
4. Nach der Bearbeitung der Einstellungen, klicken Sie auf **OK**, um die ausgeführten Änderungen zu speichern, oder auf **Abbrechen**, um sie aufzugeben.



10.2.1. Scan (Virenprüfung)

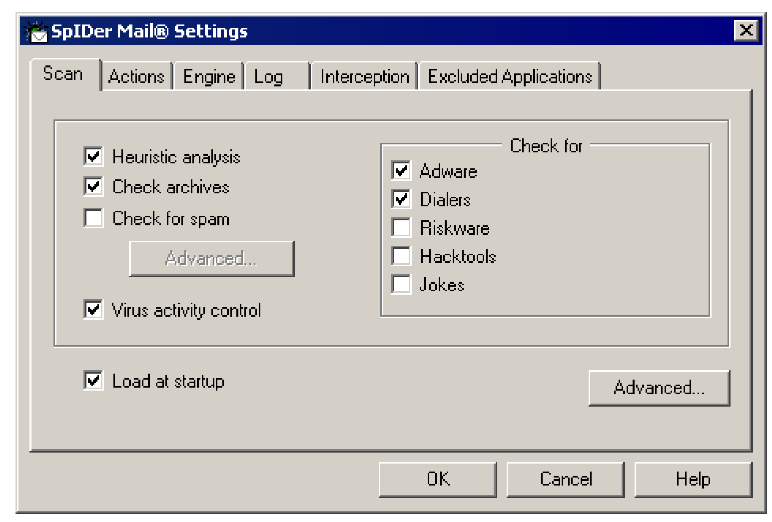


Abbildung 10-1. Einstellungsfenster von SpIDer Mail. Tab Virenprüfung.

Um Info über die Parameter in einem anderen Tab

zu erhalten, klicken Sie auf entsprechenden Tabnamen in der Abbildung

In diesem Tab wird der Prüfungsmodus für E-Mails festgesetzt.

Mit der nachfolgenden Gruppe der Einstellungen werden die Prüfparameter für E-Mails festgesetzt. Standardmäßig sind die folgenden wichtigen Einstellungen vorgegeben, deren Änderung nicht empfohlen wird:

- Das per Default gesetzte Häkchen bei **Heuristic analysis (Heuristische Analyse**) schreibt vor, dass der E-Mail-Wächter die heuristische Analyse zur Prüfung von E-Mails benutzt. In diesem Modus werden spezielle Mechanismen verwendet, die verdächtige Objekte, die mit großer Wahrscheinlichkeit mit noch unbekannten Viren infiziert sind, in E-Mails entdecken lassen.
- Das per Default gesetzte Häkchen bei **Check archives**

(Dateien in Archiven prüfen) schreibt vor, dass der Inhalt der Archive, die per E-Mail gesandt werden, geprüft wird. Um die Funktion des **SpIDer Mail** E-Mail-Wächters zu fördern, entfernen Sie das Häkchen bei **Check archives** (**Dateien in Archiven prüfen**). Damit wird diese Einstellung deaktiviert.



Der Verzicht auf die Prüfung der Archive beim permanenten Laufen des **SpIDer Guard** Wächters heisst nicht, dass Viren in den Computer eindringen. Damit wird die Entdeckung von Viren nur etwas verschoben. Beim Entpacken eines infizierten Archivs versucht das Betriebsystem, das infizierte Objekt auf die Festplatte zu schreiben. Dabei wird das schädliche Objekt vom **SpIDer Guard** Wächter entdeckt.

- Das Häkchen bei **Virus activity control** (**Kontrolle der Virusaktivität**) wird per default gesetzt. Dieser Modus schreibt vor, dass charakteristische Merkmale des Massenversandes von Viren entdeckt werden. Der Massenversand von Viren ist eine häufige Folge von Vireninfizierung des Computers. In diesem Modus kann der **SpIDer Mail** E-Mail-Wächter den E-Mail-Versand von Ihrem Computer an mehrere Adressen blockieren. Falls Probleme beim Versand von E-Mails an mehrere Empfänger entstehen, ist es empfehlenswert, dieses Häkchen zu entfernen.

In diesem Tab können Sie auch die E-Mail-Prüfung auf das Vorhandensein von unerwünschten E-Mails konfigurieren:

- Das Häkchen bei **Check for spam** (**Auf Spam prüfen**) schreibt vor, dass der E-Mail-Wächter alle eingehenden E-Mails mit Hilfe eines Spam-Filters auf Spam geprüft werden.



Die Spam-Prüfung ist nur zugänglich, wenn **Dr.Web Agent** unter Lizenz für das Programmpaket "Antivirus+Antispam" betrieben wird.

Um die Einstellungen des Spam-Filters zu ändern, klicken Sie auf den **Advanced** (**Erweitert**) Knopf unten. Es öffnet sich das Fenster Einstellungen für Spam-Prüfung der E-Mails.



Neben E-Mails mit infizierten Dateien kann der E-Mail-Wächter auch E-Mails, die andere Typen der Schadprogramme enthalten, entdecken:

- **Adware**,
- **Dialers** (**Dialer**),
- **Riskware** (**Potentiell gefährliche Software**),
- **Hacktools** (**Hackertools**),
- **Jokes** (**Scherzprogramme**).

Um den Bestand der zu entdeckenden Schadprogramme zu ändern, setzen Sie Häkchen bei den Typen der Schadprogramme, die zu entdecken sind, und löschen Sie Häkchen bei den Typen der Software, die nicht zu entdecken sind.

Standardgemäß entdeckt der E-Mail-Wächter nur **Adware** und **Dialers** (**Dialer**).



Die Reaktion des E-Mail-Wächters bei Entdeckung unerwünschter Programme stimmt mit der Reaktion auf Entdeckung von infizierten E-Mails, die im Tab Aktionen definiert wird, überein.

Das Häkchen bei **Load at startup** (**Programm-Autorun**) wird per default gesetzt. Dabei wird **SpIDer Mail** automatisch beim Windows Start gestartet. Sie können das Häkchen entfernen. In diesem Fall ist das Programm per Hand zu starten.

Zur Einstellung der zusätzlichen Parameter für E-Mail-Prüfung klicken Sie auf den Erweitert Knopf in der rechten unteren Ecke des Fensters.

10.2.1.1. Spam-Filter einstellen

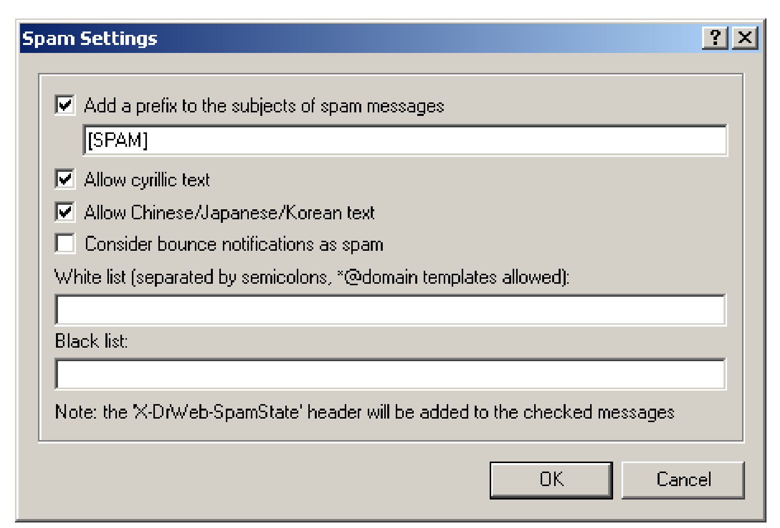


Abbildung 10-2. Einstellungsfenster von SpIDer Mail.



Wenn Sie Ihre E-Mails per IMAP/NNTP-Protokolle erhalten, stellen Sie Ihr Mail-Programm so ein, dass die E-Mails vom Mail-Server sofort und vollständig geladen werden, ohne dass E-Mail-Headers vorgeschaut werden. Dies ist zur korrekten Funktion des Spam-Filters erforderlich.

Das Häkchen bei **Add prefix to the subjects of the spam messages** (**Präfix ins Subject-Feld der E-Mails mit Spam hinzufügen**) schreibt vor, dass der **SpIDer Mail** Wächter dem Betreff der als Spam erkannten E-Mails ein spezielles Präfix hinzufügt. Das Hinzufügen des Präfixes wird Ihnen helfen, die Regeln zur Filterung der als Spam markierten E-Mails in den Mail-Clients (z.B. MS Outlook Express) zu erstellen, wo es unmöglich ist, die Filter aufgrund E-Mail-Headers einzustellen.

Das Häkchen bei **Allow Cyrillic text** (**Kyrillische Schrift erlauben**) schreibt vor, dass der Antispam-Filter die E-Mails mit eingestellter



kyrillischen Kodierung ohne vorherige Analyse nicht als Spam markiert. Wenn das Häkchen entfernt ist, werden solche E-Mails mit großer Wahrscheinlichkeit als Spam eingestuft.

Ähnlicherweise funktioniert das Setzen und Entfernen des Häkchens bei **Allow Chinese/Japanese/Korean text** (**Chinesische/ Japanische/Koreanische Schrift erlauben**).

Die Felder **White list** (**Whitelist**) und **Black list** (**Blacklist**) enthalten "schwarze" und "weiße" Adressenlisten der E-Mail-Absender.

- Wenn die Absenderadresse der Whitelist hinzugefügt wird, wird die E-Mail auf Spam nicht geprüft. Wenn aber die Domain-Namen der Empfänger- und Absenderadressen gleich sind und dieser Domain-Name in die Whitelist mit der "*" Maske eingetragen ist, so wird die E-Mail auf Spam geprüft.

  Eingabemethoden

  - um einen bestimmten Absender in die Liste hinzuzufügen, geben Sie seine komplette E-Mail-Adresse (z.B. `mail@example.net`) an. Alle E-Mails, die von dieser Adresse erhalten werden, werden ohne Spam-Prüfung zugestellt;
  - unterschiedliche E-Mail-Adressen werden mit dem ";" Zeichen voneinander getrennt;
  - um die E-Mail-Adressen bestimmter Art in die Absenderliste hinzuzufügen, geben Sie eine Maske, die diese Adressen definiert, ein. Die Maske setzt das Template zur Definition des Objektes fest. Sie kann übliche Zeichen, die in E-Mail-Adressen erlaubt sind, sowie das spezielle * Zeichen, mit dem eine beliebige (auch leere) Zeichenfolge ersetzt werden kann, beinhalten.

    Beispielsweise sind folgende Varianten möglich:

    - `mailbox@domain.com`
    - `*box@domain.com`
    - `mailbox@dom*`
    - `*box@dom*`





Das * Zeichen wird nur am Anfang oder am Ende der E-Mail-Adresse gesetzt.

Das @ Zeichen ist obligatorisch.

- um E-Mails von E-Mail-Adressen einer bestimmten Domain garantiert zu erhalten, benutzen Sie das * Zeichen anstatt des Benutzernamens. Um alle E-Mails z.B. von Adressaten auf der `example.net` Domain zu erhalten, geben Sie `*@example.net` ein;
- um E-Mails von E-Mail-Adressen mit einem bestimmten Benutzernamen von einer beliebigen Domain garantiert zu erhalten, benutzen Sie das * Zeichen anstatt des Domain-Namens. Um alle E-Mails z.B. von Adressaten mit dem Namen des E-Mail-Postfaches "ivanov" zu erhalten, geben Sie `ivanov@*` ein.

- Wenn die Absenderadresse der Blacklist hinzugefügt wird, wird die E-Mail ohne zusätzliche Analyse als Spam eingestuft.

Eingabemethoden

- um einen bestimmten Absender in die Liste hinzuzufügen, geben Sie seine komplette E-Mail-Adresse (z.B. `spam@spam.ru`) an. Alle E-Mails, die von dieser Adresse erhalten werden, werden automatisch als Spam eingestuft;
- unterschiedliche E-Mail-Adressen werden mit dem ";" Zeichen voneinander getrennt;
- um die E-Mail-Adressen bestimmter Art in die Absenderliste hinzuzufügen, geben Sie eine Maske, die diese Adressen definiert, ein. Die Maske setzt das Template zur Definition des Objektes fest. Sie kann übliche Zeichen, die in E-Mail-Adressen erlaubt sind, sowie das spezielle * Zeichen, mit dem eine beliebige (auch leere) Zeichenfolge ersetzt werden kann, beinhalten.

  Beispielsweise sind folgende Varianten möglich:

  - `mailbox@domain.com`
  - `*box@domain.com`
  - `mailbox@dom*`



- `*box@dom*`



Das `*` Zeichen wird nur am Anfang oder am Ende der E-Mail-Adresse gesetzt.

Das `@` Zeichen ist obligatorisch.

- um E-Mails von E-Mail-Adressen einer bestimmten Domain als Spam garantiert zu markieren, benutzen Sie das `*` Zeichen anstatt des Benutzernamens. Um alle E-Mails z.B. von Adressaten auf der `spam.ru` Domain als Spam zu markieren, geben Sie `*@spam.ru` ein;
- um E-Mails von E-Mail-Adressen mit einem bestimmten Benutzernamen von einer beliebigen Domain als Spam garantiert zu markieren, benutzen Sie das `*` Zeichen anstatt des Domain-Namens. Um alle E-Mails z.B. von Adressaten mit dem Namen des E-Mail-Postfaches "ivanov" als Spam zu markieren, geben Sie `ivanov@*` ein;
- die E-Mail-Adressen auf Domain des Empfängers werden nicht bearbeitet. Falls die E-Mail-Adresse des Empfängers (Ihre E-Mail-Adresse) beispielsweise auf der `mail.ru` Domain eingerichtet wurde, so werden die Absenderadressen der `mail.ru` Domain vom Spam-Filter nicht bearbeitet.

Alle geprüften E-Mails erhalten Headers:

- **X-DrWeb-SpamState: Yes/No**. Der Wert **Yes** weist darauf hin, dass die E-Mail als Spam eingestuft wurde, **No** – die E-Mail ist nach **SpIDer Mail** kein Spam.
- **X-DrWeb-SpamVersion: version**. **version** – Version der Bibliothek vom **Vade Retro** Antispam-Filter.





Wenn manche E-Mails vom Spam-Filter falsch eingestuft werden, sollen diese an spezielle E-Mail-Adressen zur Analyse und Leistungserhöhung des Spam-Filters gesandt werden. Die als Spam falsch markierte E-Mails sind an vrnonspam@drweb.com zu senden. Spam-E-Mails, die vom System nicht erkannt wurden, senden Sie bitte an vrspam@drweb.com. Alle Nachrichten sind nur im Anhang (nicht im E-Mail-Körper) zu senden.

10.2.1.2. Zusätzliche Einstellungen des Prüfungsmodus

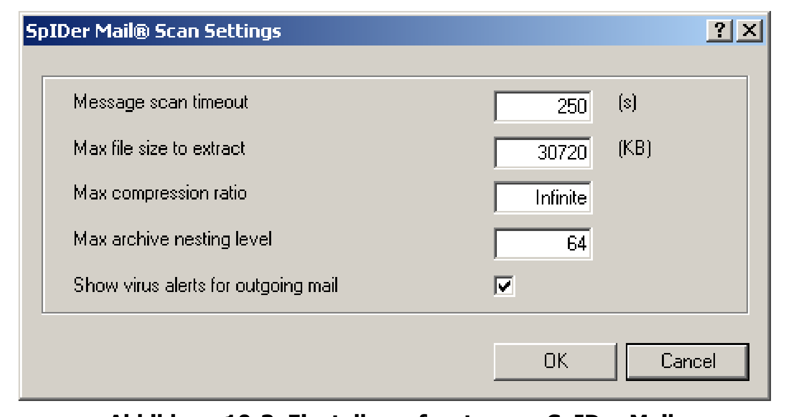


Abbildung 10-3. Einstellungsfenster von SpIDer Mail.

In diesem Fenster werden die zusätzlichen Einstellungen für E-Mail-Prüfung festgesetzt.

Die nachfolgende Gruppe der Einstellungen setzt Bedingungen fest, bei deren Ausführung die kompliziert aufgebauten E-Mails, deren Prüfung äußerst aufwändig ist, als nicht geprüft definiert werden:

- **Message scan timeout** (**Timeout bei E-Mail-Prüfung**) – maximale Zeit, innerhalb der eine E-Mail geprüft wird. Nach Ablauf dieser Zeit wird die Prüfung abgebrochen;
- **Max file size to extract** (**Max. Länge der Datei beim**



Entpacken) – wenn der E-Mail-Wächter feststellt, dass das Archiv nach dem Entpacken länger als angegeben wird, werden weder Prüfung noch Entpacken ausgeführt;

- **Max compression ratio** (**Max. Komprimierung des Archivs**) – wenn der E-Mail-Wächter feststellt, dass der Komprimierungsgrad den angegebenen Wert übersteigt, werden weder Entpacken noch Prüfung ausgeführt;
- **Max archive nesting level** (**Max. Verschachtelung des Archivs**) – wenn die Verschachtelungstiefe den angegebenen Wert übersteigt, wird die Prüfung nur bis zur angegebenen Verschachtelungstiefe ausgeführt.

Das Häkchen bei **Show virus alerts for outgoing mail flag** (**Vor Viren in ausgehenden E-Mails warnen**) wird per default gesetzt. Dabei öffnet sich ein Meldefenster, das über den fehlgeschlagenen Versand einer infizierten E-Mail an SMTP-Server benachrichtigen wird. In der Regel wird eine ähnliche Nachricht vom Mail-Programm erstellt; in diesem Fall kann das Häkchen entfernt werden.



10.2.2. Actions (Aktionen)

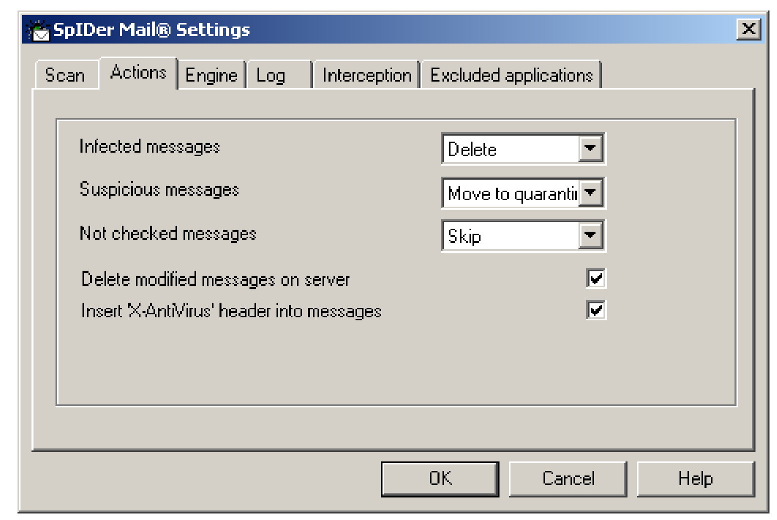


Abbildung 10-4. Einstellungsfenster von SpIDer Mail. Tab Aktionen. Um Info über die Parameter in einem anderen Tab zu erhalten, klicken Sie auf entsprechenden Tabnamen in der Abbildung

In diesem Tab werden die Reaktionen des **SpIDer Mail** Wächters bei Entdeckung von infizierten oder verdächtigen Dateien in E-Mails festgesetzt.

Aktionen einstellen

Folgende Einstellungen dienen zur Festsetzung von Aktionen bei entdeckten schädlichen Objekten:

- Die ausfallende Liste **Infected messages** (**Infizierte E-Mails**) setzt die Reaktion von **SpIDer Mail** bei Entdeckung einer E-Mail, die das schädliche Objekt enthält, fest.
- Die ausfallende Liste **Suspicious messages** (**Verdächtige E-Mails**) setzt die Reaktion von **SpIDer Mail** bei Entdeckung

einer E-Mail, die vermutlich ein Virus enthält (Ergebnis der heuristischen Analyse), fest.

- Die ausfallende Liste **Not checked messages** (**Nicht geprüfte E-Mails**) setzt die Reaktion von **SpIDer Mail** bei Entdeckung der E-Mails, deren Prüfung nicht beendet werden konnte.

Das Häkchen bei **Delete modified messages on server (Modifizierte E-Mails auf dem Server löschen**) wird per default gesetzt. In diesem Fall werden alle eingehenden E-Mails, für die Reaktion **Delete** (**Löschen**) oder **Quarantine** (**In Quarantäne**) verwendet wurde, unabhängig von Einstellungen des Mail-Clients vom POP3/IMAP4-Server gelöscht.

Wird das Häkchen bei **Insert 'X-AntiVirus' header into messages** (**'X-AntiVirus' Header den Nachrichten hinzufügen**) gesetzt, so erhalten alle geprüften E-Mails folgende Headers:

- **X-DrWeb-SpamState: Yes/No**. Der Wert **Yes** weist darauf hin, dass die E-Mail als Spam eingestuft wurde, **No** – die E-Mail ist nach **SpIDer Mail** kein Spam.
- **X-DrWeb-SpamVersion: version**. **version** – Version der Bibliothek vom Vade Retro Antispam-Filter.

Mögliche Reaktionen

Bei entdeckten Objekten sind folgende Aktionen möglich:

- **Delete** (**Löschen**) – in diesem Fall übermittelt der E-Mail-Wächter dem E-Mail-Client keine Mail. Statt der gelöschten E-Mail erhält das E-Mail-Client eine Nachricht über die ausgeführte Aktion.
- **Quarantine** (**In Quarantäne**) – in diesem Fall wird die E-Mail dem E-Mail-Client nicht übermittelt, sondern in den Quarantäne-Ordner verschoben. Statt der verschobenen E-Mail erhält das E-Mail-Client eine Nachricht über die ausgeführte Aktion.
- **Skip** (**Überspringen**) – die E-Mails werden dem E-Mail-Client üblicherweise übermittelt.



Bei ausgehenden E-Mails haben diese Aktionen (außer **Überspringen**) den Verzicht auf E-Mail-Versand an SMTP-Server zur Folge.

Tabelle 7. SpIDer Mail Aktionen bei E-Mail-Prüfung

Objekt	Aktion		
	Löschen	In Quarantäne	Überspringen
Infizierte E-Mails	+	+/*	
Verdächtige E-Mails	+	+/*	+
Nicht geprüfte E-Mails	+	+	+/*

Symbole

+	die Aktion ist für diesen Typ der Objekte freigegeben
+/*	die Aktion ist als standardmäßige Reaktion für diesen Typ der Objekte festgesetzt

10.2.3. Engine

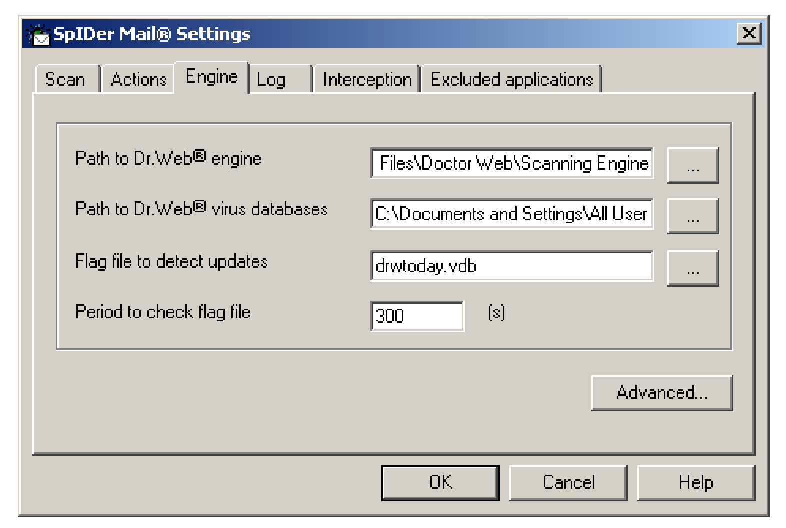


Abbildung 10-5. Einstellungsfenster von SpIDer Mail. Tab Engine. Um Informationen über Parameter in einem anderen Tab zu erhalten, klicken Sie auf den entsprechenden Tabnamen in der Abbildung

In diesem Tab werden die Parameter der Antivirus-Engine eingestellt.

Gegebenenfalls können Sie benutzerdefinierte Anordnung der Antivirus-Engine (der Suchengine) und der Virendatenbanken festlegen.

Wenn während der Sitzung des Wächters die Virendatenbanken mit Hilfe des **Aktualisierungsmoduls** aktualisiert wurden, lädt der Wächter sofort die aktualisierten Virendatenbanken herunter. Wenn die Aktualisierung von Virendatenbanken anders durchgeführt wurde (z.B. durch das direkte Kopieren der Virendatenbanken in den Installationsordner), kann der Wächter die aktualisierten Virendatenbanken auch ohne Neustart des Programms herunterladen. Dazu dient der Mechanismus der periodischen Prüfung der Referenzdatei. Die Änderung der Referenzdatei informiert über die

Notwendigkeit des Neuladens der Virendatenbanken. Sie können den Namen und Pfad der Referenzdatei sowie den Zeitabstand zwischen den Prüfungen (standardgemäß 300 Sekunden) festsetzen.

Klicken Sie auf **Advanced** (**Erweitert**), um zusätzliche Einstellungen der Antivirus-Engine festzusetzen.

10.2.3.1. Zusätzliche Einstellungen der Suchengines

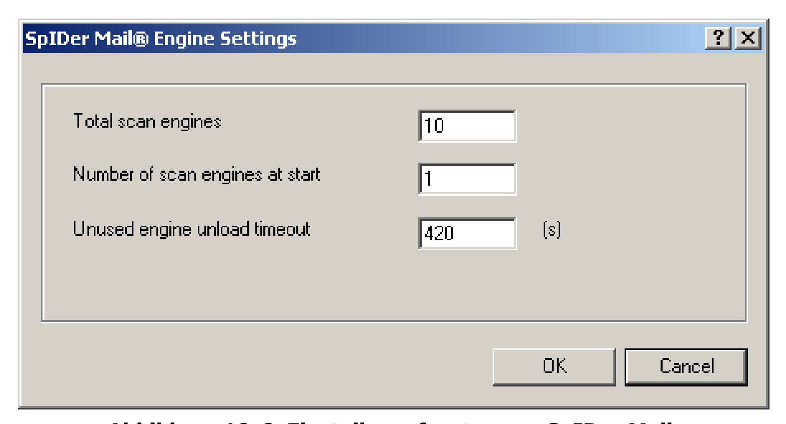


Abbildung 10-6. Einstellungsfenster von SpIDer Mail.

In diesem Fenster werden die zusätzlichen Einstellungen für Suchengine festgesetzt:

- Im Feld **Total scan engines** (**Gesamtanzahl der Suchengines**) wird die maximale Anzahl der gleichzeitig geladenen Suchengines festgesetzt.
- Im Feld **Numbers of scan engines at start** (**Anzahl der Suchengines beim Starten**) wird die Anzahl der Suchengines, die beim Starten von **SpIDer Mail** geladen werden, festgesetzt.
- Im Feld **Unused engines unload timeout** (**Freie Suchengines deaktivieren in**) wird die Zeit in Sekunden festgesetzt, nach deren Ablauf eine nicht benutzte Suchengine deaktiviert wird.

10.2.4. Log (Protokoll)

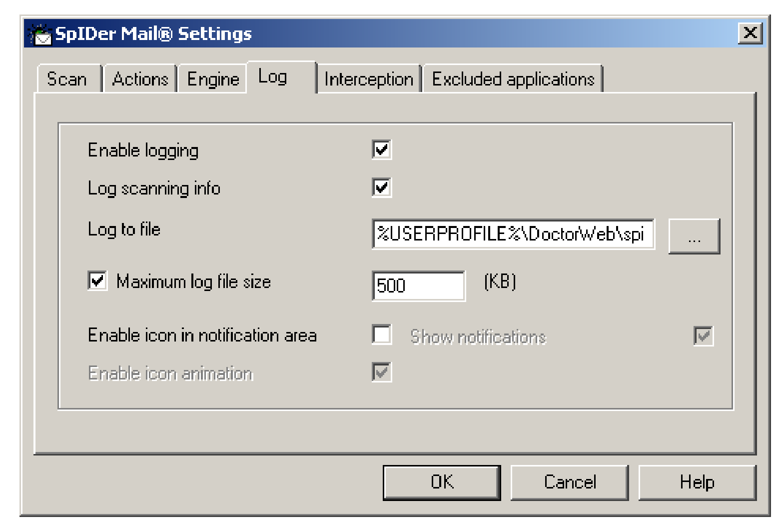


Abbildung 10-7. Einstellungsfenster von SpIDer Mail. Tab Protokoll. Um Informationen über Parameter in einem anderen Tab zu erhalten, klicken Sie auf den entsprechenden Tabnamen in der Abbildung

In diesem Tab werden die Parameter der Protokolldatei von **SpIDer Mail** festgelegt.

Das Häkchen bei **Enable logging** (**Protokoll führen**) schreibt vor, dass der **SpIDer Mail** Wächter die Protokolldatei führt. Standardgemäß wird das Häkchen gesetzt.

Sie können folgende Parameter der Protokolldatei einstellen:

- Setzen Sie ein Häkchen bei **Log scanning info** (**Protokoll über geprüfte Objekte**), um die Angaben über alle geprüften Objekte, eingeschlossen von nicht infizierten Objekten, ins Protokoll einzutragen.
- Im Feld **Log to file** (**Protokolldatei führen**) können Sie den Namen und den Pfad der Protokolldatei eingeben. Klicken Sie auf



den [...] Knopf, um das Objekt im Dateibrowser des Betriebssystems anzugeben.

- Setzen Sie ein Häkchen bei **Maximum log file size (Maximale Größe der Protokolldatei)**, um die maximale Größe der Protokolldatei einzuschränken, und geben Sie die maximal zulässige Größe in Kilobytes an.

Sie können auch die zusätzlichen Parameter festsetzen:

- Setzen Sie ein Häkchen bei **Enable icon in the notification area** (**Programm-Icon anzeigen**), damit das Icon von **SpIDer Mail** im Infobereich der Taskleiste angezeigt wird.
- Setzen Sie ein Häkchen bei **Enable icon animation (Animiertes Icon**) anzeigen, damit das animierte Icon von **SpIDer Mail** im Infobereich der Taskleiste angezeigt wird.
- Setzen Sie ein Häkchen bei **Show notifications (Benachrichtigungen anzeigen**), damit eine Popup-Tippbenachrichtigung mit der Information über Programmversion,Anzahl der Vireneinträge usw. über dem **SpIDer Mail** Icon angezeigt wird. Die Tippbenachrichtigung erscheint gleich nach dem Programmstart.

10.2.5. Interception (Abfangen)

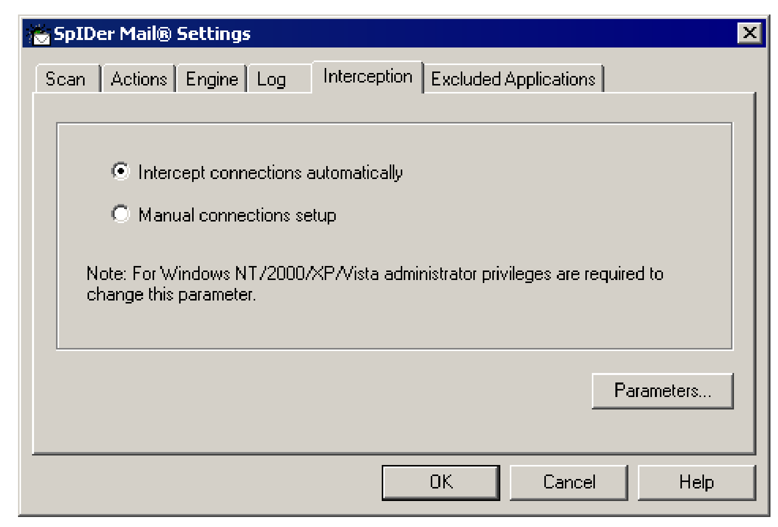


Abbildung 10-8. Einstellungsfenster von SpIDer Mail. Tab Abfangen. Um Informationen über Parameter in einem anderen Tab zu erhalten, klicken Sie auf den entsprechenden Tabnamen in der Abbildung

In diesem Tab werden die Parameter des Abfangens von Verbindungen zu den POP3/SMTP/IMAP4/NNTP-Servern festgesetzt.

Wählen Sie den Abfangmodus aus:

- automatischer Modus ist meist komfortabel;
- manueller Modus ist nur dann zu verwenden, wenn der automatische Modus für alle oder einige abzufangenden Serveradressen unmöglich ist (für alle Adressen soll ein und derselbe Modus verwendet werden).

Nachdem der Modus ausgewählt ist, klicken Sie auf **Parameters (Parameter**). Es öffnet sich das Fenster, in dem das Abfangen im ausgewählten Modus eingestellt werden kann.

10.2.5.1. Automatisches Abfangen

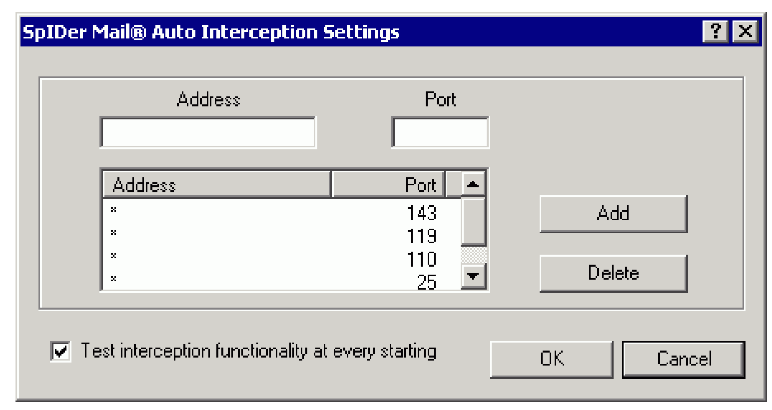


Abbildung 10-9. Einstellungsfenster des automatischen Abfangens von SpIDer Mail.

In diesem Fenster werden die Einstellungen für das Abfangen im automatischen Modus festgesetzt.

Die Liste der abzufangenden Adressen der Mail-Server enthält standardgemäß vier Elemente:

- beliebige Adressen auf Port 143 – standardmäßige IMAP4-Server,
- beliebige Adressen auf Port 119 – standardmäßige NNTP-Server,
- beliebige Adressen auf Port 110 – standardmäßige POP3-Server,
- beliebige Adressen auf Port 25 – standardmäßige SMTP-Server.

Sie können diese Liste editieren:

1. Um ein Element in die Liste hinzuzufügen, geben Sie entsprechende Daten in den Feldern **Address** (**Adresse**) und **Port** an und klicken Sie auf **Add** (**Hinzufügen**).
2. Um ein Element aus der Liste zu entfernen, markieren dieses Element in der Liste und klicken Sie auf **Delete** (**Löschen**).



Das standardgemäß gesetzte Häkchen bei **Test interception functionality at every starting** (**Abfangen von Verbindungen beim Starten prüfen**) schreibt vor, dass das Programm die Funktion des automatischen Abfangs prüft. Wenn der automatische Abfang wenigstens einer Verbindung unmöglich ist, wechseln Sie zum manuellen Abfangmodus.

10.2.5.2. Manuelles Abfangen

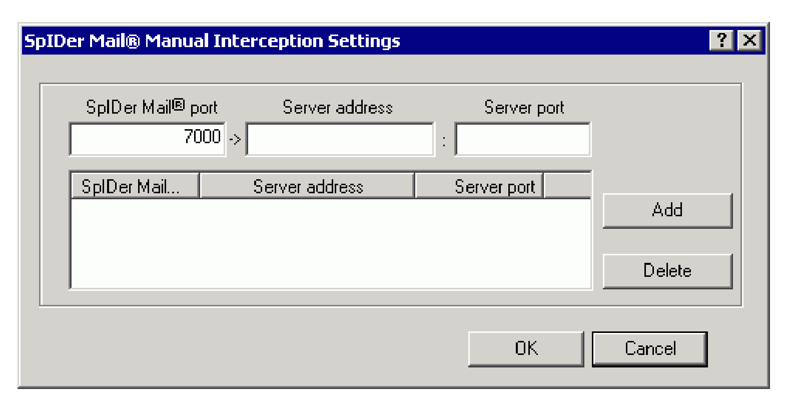


Abbildung 10-10. Einstellungsfenster des manuellen Abfangens von SpIDer Mail.

In diesem Fenster werden die Einstellungen des manuellen Abfangs von Verbindungen zu den Mail-Servern festgesetzt. In diesem Modus tritt der **SpIDer Mail** E-Mail-Wächter als ein Proxy-Server zwischen den Mail-Programmen und Mail-Servern auf. Der Wächter prüft nur die Verbindungen, die in den Einstellungen explizit angegeben sind. Deswegen erfordert die Nutzung von diesem Typ des Abfangens, dass die Änderung von Einstellungen für Verbindung der Mail-Programme ausgeführt wird.

Die Liste der abzufangenden Adressen enthält Einträge, von denen jeder jeweils die Übereinstimmung der Einstellungen zwischen dem **SpIDer Mail** E-Mail-Wächter und dem Mail-Server definiert.

Standardgemäß ist die Abfangliste leer. Sie können hier erforderliche Einträge machen.

Den manuellen Abfangmodus einstellen

1. Erstellen Sie die Liste der Mail-Server, zu welchen Sie die Verbindungen abfangen wollen, und geben Sie die Portnummern für diese Server aufsteigend und lückenlos an. Es empfiehlt sich, die Nummerierung mit der 7000 anzufangen. Im weiteren werden diese Nummern *SpIDer Mail Ports* genannt.



Der **SpIDer Mail** E-Mail-Wächter uterstüzt die Mail-Server, die über POP3, SMTP, IMAP4 oder NNTP Protokolle funktionieren.

2. In den Einstellungen des **SpIDer Mail** E-Mail-Wächters wählen Sie den Abschnitt **Interception** (**Abfangen**).
3. Wählen Sie den manuellen Abfangmodus aus und klicken Sie auf **Connection Settings** (**Verbindungseinstellungen**).
4. Im geöffneten Dialogfenster geben Sie folgende Informationen ein:
    - im Feld **SpIDer Mail Port** – *SpIDer Mail Port*, der für Mail-Server ausgewählt wurde;
    - im Feld **Server address** – Domainname oder IP-Adresse des Mail-Servers;
    - im Feld **Server port** – Nummer des Ports, der vom Mail-Server benutzt wird.
5. Klicken Sie auf **Add** (**Hinzufügen**).
6. Gegebenenfalls wiederholen Sie die Schritte 4 und 5 für andere Server. Um das Abfangen von Verbindungen zum Server zu stoppen, wählen Sie das entsprechende Element in der Liste aus und klicken Sie auf **Remove** (**Löschen**).
7. Nach der Bearbeitung der Einstellungen, klicken Sie auf **OK**, um die Änderungen zu speichern, oder auf **Cancel (Abbrechen**), um sie zu verwerfen.
8. Konfigurieren Sie Ihren Mail-Client für das Zusammenwirken mit dem **SpIDer Mail** E-Mail-Wächter beim manuellen Abfangen von Verbindungen.



Mail-Client einstellen

Wenn die manuellen Einstellungen für das Abfangen von Verbindungen vom **SpIDer Mail** verwendet werden, dann ändern Sie die Einstellungen Ihres Mail-Clients wie folgt:

- als Serveradresse für eingehende und ausgehende E-Mails geben Sie `localhost` an;
- als Port des Mail-Servers geben Sie den *SpIDer Mail Port* an, den Sie für entsprechenden Mail-Server festgesetzt haben.

In der Regel müssen Sie dafür in den Einstellungen der Mail-Server-Adresse folgendes angeben:

`localhost`: **<***SpIDer_Mail_Port***>**

wo <*SpIDer_Mail_Port*> – der Port, den Sie für entsprechenden Mail-Server festgesetzt haben.

Zum Beispiel

Wenn der Mail-Server mit der `pop.mail.ru` Adresse und dem Port 110 auf *SpIDer Mail Port* 7000 festgesetzt wurde, ist es notwendig, `localhost` als Server für eingehende E-Mails und `7000` als Port in den Einstellungen des Mail-Clients anzugeben.



10.2.6. Excluded Applications (Ausgenommene Anwendungen)

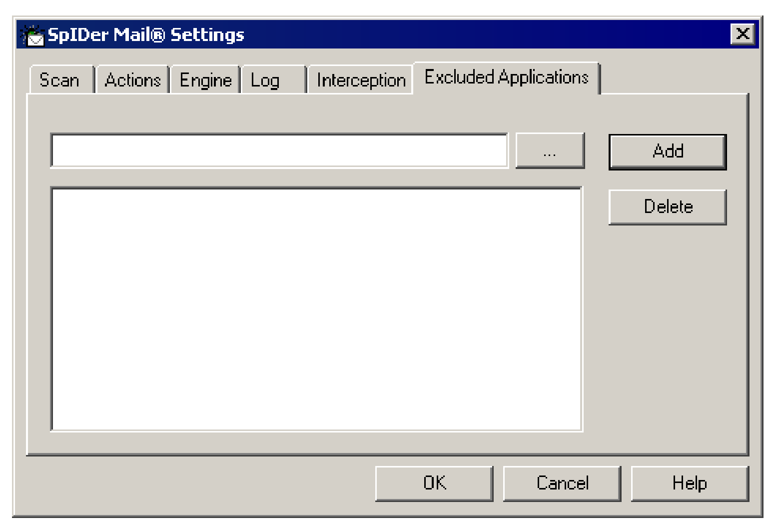


Abbildung 10-11. Einstellungsfenster von SpIDer Mail. Tab Ausgenommene Anwendungen.

Um Informationen über Parameter in einem anderen Tab zu erhalten, klicken Sie auf den entsprechenden Tabnamen in der Abbildung

In diesem Tab wird die Liste der Anwendungen festgesetzt, deren Mail-Verkehr nicht abgefangen und dementsprechend vom E-Mail-Wächter nicht analysiert wird.

Um die Liste der Anwendungen einzustellen:

1. Geben Sie den Pfad der ausführbaren Anwendungsdatei ein. Sie können auch den ... Knopf benutzen und das Objekt im Datei-Browser des Betriebssystems auswählen.
2. Klicken Sie auf **Add** (**Hinzufügen**). Die Anwendung wird in die unten angeordnete Liste hinzugefügt.



3. Um eine Anwendung aus der Liste zu entfernen, wählen Sie seine ausführbare Datei in der Liste aus und klicken Sie auf **Delete** (**Löschen**).



Kapitel 11. Dr.Web für Outlook

Grundfunktionen der Komponente

Das anzuschließende **Dr.Web für Outlook** Modul führt folgende Funktionen aus:

- Virenprüfung der an E-Mails angehängten Dateien.
- Prüfung der E-Mails, die über eine verschlüsselte SSL-Verbindung versandt werden.
- Spam-Prüfung der E-Mails.
- Erkennung und Neutralisierung der schädlichen Software.
- Verwendung der heuristischen Analyse zum zusätzlichen Schutz vor unbekannten Viren.

Aktivieren/Deaktivieren

Das Aktivieren und Deaktivieren des **Dr.Web für Outlook** Moduls erfolgt über das Kontextmenü des **Agenten**.

Das Modul Dr.Web für Outlook einstellen

Zur Einstellung der Parameter sowie zum Anschauen von Programmstatistik gehen Sie zu Microsoft Outlook, Abschnitt **Extras** → **Optionen** → Tab **Dr.Web Antivirus**.



Der zu Einstellungen von Microsoft Outlook gehörende **Dr. Web Anti-Virus** Tab ist nur zugänglich, wenn der Benutzer die Rechte, die diese Einstellungen ändern lassen, besitzt. Die Rechte werden vom Administrator des Antivirus-Netzwerkes auf dem **Server** festgelegt.



Abbildung 11-1. Einstellungsfenster von Microsoft Outlook. Dr.Web Antivirus Tab.

Im Tab **Dr.Web Antivirus** wird der aktuelle Schutzstatus (aktiviert/ deaktiviert) angezeigt sowie Zugriff auf folgende Programmoptionen sichergestellt:

- Protokoll - lässt die Registrierung der Programm-Ereignisse einstellen;
- Anhänge prüfen - lässt die E-Mail-Prüfung einstellen sowie Aktionen des Programms für entdeckte schädliche Objekte

definieren;

- Spam-Filter - lässt Aktionen des Programms bei Spam-Nachrichten festsetzen sowie White- und Blacklists von E-Mails erstellen;
- Statistik - zeigt Angaben zu Objekten, die vom Programm geprüft und bearbeitet wurden.

11.1. Virenprüfung

Dr.Web für Outlook nutzt unterschiedliche Entdeckungsverfahren von Viren. Gegen gefundene schädliche Objekte werden benutzerdefinierte Aktionenverwendet: infizierte Objekte können vom Programm desinfiziert, gelöscht oder in Quarantäne zur Isolierung und zuverlässigen Speicherung verschoben werden.

11.1.1. Schädliche Objekte

Das Programm **Dr.Web für Outlook** entdeckt folgende böswillige Objekte:

- infizierte Archive;
- Datei-Bomben und Archivbomben;
- Adware;
- Hackertools;
- Dialer;
- Scherzprogramme;
- potentiell verdächtige Software.

11.1.2. Aktionen

Dr.Web für Outlook lässt die Reaktion des Programms bei Entdeckung von infizierten oder verdächtigen Dateien und Schadprogrammen in E-Mail-Anhängen einstellen.



Um die Prüfung der Anhänge einzustellen und die Aktionen des Programms bei entdeckten schädlichen Objekten zu definieren, gehen Sie zu Microsoft Outlook, Abschnitt **Extras** → **Optionen** → Tab **Dr. Web Antivirus** und klicken Sie auf **Anhänge prüfen**.

Anhänge prüfen

Scan-Einstellungen

Infiziert	Desinfizieren
Nicht desinfiziert	In Quarantäne verschieben
Verdächtig	In Quarantäne verschieben
Malware	
Adware	In Quarantäne verschieben
Dialer	In Quarantäne verschieben
Scherzprogramme	In Quarantäne verschieben
Hackertools	In Quarantäne verschieben
Riskware	In Quarantäne verschieben
Wenn die Prüfung	In Quarantäne verschieben

☑ Archive prüfen (empfehlenswert)

OK | Abbrechen | Übernehmen

Abbildung 11-2. Einstellungsfenster der Anhangprüfung.



Das Fenster **Anhänge prüfen** ist nur zugänglich, wenn der Benutzer Systemadministratorrechte besitzt.

Wenn Sie unter Windows Vista und neuer auf **Anhänge prüfen** klicken:

- Bei aktivierter UAC: der Administrator erhält eine Aufforderung zur Bestätigung von Programmaktionen. Der Benutzer ohne Administratorrechte erhält eine Aufforderung zur Eingabe von Identifiezierungsdaten des Systemadministrators.
- Bei deaktivierter UAC: der Administrator kann Programmeinstellungen ändern. Der Benutzer erhält keinen Zugriff auf Änderung von Einstellungen.

Im Fenster **Anhänge prüfen** können Sie die Aktionen des Programms bei unterschiedlichen Kategorien der zu prüfenden Objekte sowie für den Fall, dass Fehler während der Prüfung aufgetreten sind, festsetzen. Sie können auch die Prüfung der Archive einstellen.

Zur Definition der Aktionen für entdeckte schädliche Objekte dienen folgende Einstellungen:

- Die ausfallende Liste **Infiziert** setzt die Reaktion auf Entdeckung der Objekte, die mit bekannten und (vermutlich) desinfizierbaren Viren infiziert sind.
- Die ausfallende Liste **Nicht desinfiziert** setzt die Reaktion auf Entdeckung der Objekte, die mit einem bekannten, nicht desinfizierbaren Virus infiziert sind, eingeschlossen der Desinfektionsversuche, die fehlgeschlagen sind.
- Die ausfallende Liste **Verdächtige** setzt die Reaktion auf Entdeckung der Objekte, die mit einem Virus vermutlich infiziert sind (Ergebnis der heuristischen Analyse).
- Der Abschnitt **Malware** setzt die Reaktion auf Entdeckung folgender unerwünschter Software:
    - Adware;
    - Dialer;
    - Scherzprogramme;
    - Hackertools;
    - Riskware.
- Die ausfallende Liste **Wenn die Prüfung** lässt die Aktionen des Programms für den Fall einstellen, dass die Prüfung eines Anhangs unmöglich ist, z.B. wenn der Anhang eine beschädigte oder mit Passwort geschützte Datei ist.



- Das Häkchen bei **Archive prüfen** lässt die Prüfung der als Archiv angehängten Dateien aktivieren oder deaktivieren. Setzen Sie dieses Häkchen zur Aktivierung der Prüfung. Um die Prüfung zu deaktivieren, entfernen Sie das Häkchen.

Die verfügbaren Reaktionen unterscheiden sich je nach dem Typ des Virenereignisses.

Folgende Aktionen können für gefundene Objekte ausgeführt werden:

- **Desinfizieren** - heisst, dass das Programm versucht, das infizierte Objekt zu desinfizieren;
- **Wie für nicht desinfizierte** - heisst, dass eine für nicht desinfizierte Objekte festgelegte Aktion gegen infizierten Anhang verwendet wird;
- **Löschen** - das Objekt aus dem System löschen;
- **In Quarantäne verschieben** - das Objekt im Quarantäne-Ordner isolieren;
- **Überspringen** - das Objekt ohne Änderungen überspringen.

Tabelle 8. Aktionen bei entdeckten schädlichen Objekten

Objekt	Aktion				
	Desin-fizieren	Wie für nicht desinfizierte	Löschen	In Quarantäne verschieben	Übersprin-gen
Infiziert	+/*	+			
Nicht desinfiziert			+	+/*	
Verdächtig			+	+/*	+
Adware			+	+/*	+
Dialer			+	+/*	+
Scherzprogramme			+	+/*	+
Hackertools			+	+/*	+
Riskware			+	+/*	+



Objekt	Aktion				
	Desin-fizieren	Wie für nicht desinfizierte	Löschen	In Quarantäne verschieben	Übersprin-gen
Wenn die Prüfung			+	+/*	+

Symbole

+	Die Aktion ist für diesen Typ der Objekte freigegeben
+/*	Die Aktion ist als standardmäßige Reaktion für diesen Typ der Objekte festgesetzt

11.2. Spam-Prüfung

Dr.Web für Outlook prüft alle E-Mails mit Hilfe des **Vade Retro** Spam-Filters auf Spam und filtert Nachrichten gemäß den Einstellungen, die vom Benutzer definiert werden.

Um die Spam-Prüfung der E-Mails einzustellen, gehen Sie zu Microsoft Outlook, Abschnitt **Extras** → **Optionen** → Tab **Dr.Web Antivirus** und klicken Sie auf **Spam-Filter**. Es öffnet sich das Einstellungsfenster des Spam-Filters.



Der Abschnitt **Spam-Filter** ist nur zugänglich, wenn **Dr. Web Agent** unter Lizenz für das Programmpaket "Antivirus+Antispam" betrieben wird.

Falls die Lizenz den Spam-Filter nicht unterstützt, werden die Einstellungen der Spam-Prüfung unzugänglich sein. Die Spam-Prüfung der Nachrichten wird nicht ausgeführt.



Das Fenster **Spam-Filter** ist nur zugänglich, wenn der Benutzer die Systemadministratorrechte besitzt.

Wenn Sie unter Windows Vista und neuer auf **Spam-Filter** klicken:



- Bei aktivierter UAC: der Administrator erhält eine Aufforderung zur Bestätigung von Programmaktionen. Der Benutzer ohne Administratorrechte erhält eine Aufforderung zur Eingabe von Identifiezierungsdaten des Systemadministrators.
- Bei deaktivierter UAC: der Administrator kann Programmeinstellungen ändern. Der Benutzer erhält keinen Zugriff auf Änderung von Einstellungen.

11.2.1. Spam-Filter einstellen

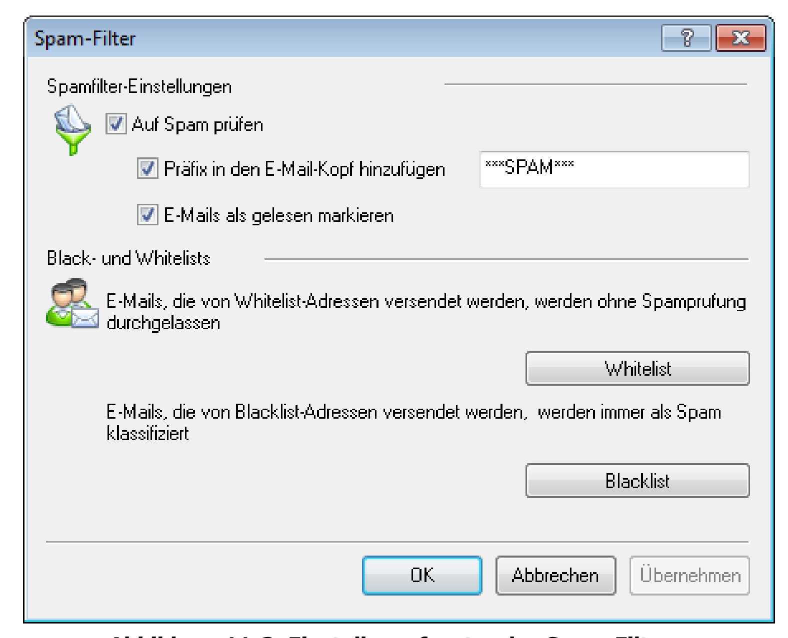


Abbildung 11-3. Einstellungsfenster des Spam-Filters.

Um die Parameter des Spam-Filters einzustellen:

- Setzen Sie ein Häkchen bei **Auf Spam prüfen** zur Aktivierung des Spam-Filters.
- Wenn Sie speziellen Text dem Header einer Nachricht, die als

Spam markiert wurde, hinzufügen möchten, setzen Sie das Häkchen bei **Präfix in den E-Mail-Kopf hinzufügen**. Das Feld zur Texteingabe befindet sich rechts vom Häkchen. Standardgemäß wird das *****SPAM***** Präfix hinzugefügt.

- Die geprüften Nachrichten können als gelesen in Eigenschaften der E-Mail markiert werden. Dafür setzen Sie ein Häkchen bei **E-Mails als gelesen markieren.** Standardgemäß wird das Häkchen bei **E-Mails als gelesen markieren** gesetzt.
- Sie können auch die White- und Blacklists zur Filterung der E-Mails einstellen.



Wenn manche E-Mails falsch eingestuft werden, sollen diese an spezielle E-Mail-Adressen zur Analyse und Leistungserhöhung des Spam-Filters gesandt werden.

Mehr dazu

- Nachrichten, die fälschlicherweise als Spam erkannt wurden, sind an folgende Adresse zu senden: vrnonspam@drweb.com;
- Nicht erkannte und versäumte Spam-Nachrichten sind an folgende Adresse zu senden: vrspam@drweb.com.

Alle Nachrichten sind nur im Anhang (nicht im E-Mail-Körper) zu senden.

11.2.2. Black- und Whitelists

Die Black- und Whitelists der E-Mail-Adressen dienen zum Filtern von Nachrichten.

Zum Ansehen und Bearbeiten des Black- oder Whitelists klicken Sie dementsprechend auf **Blacklist** oder **Whitelist** in den Einstellungen des Spam-Filters.

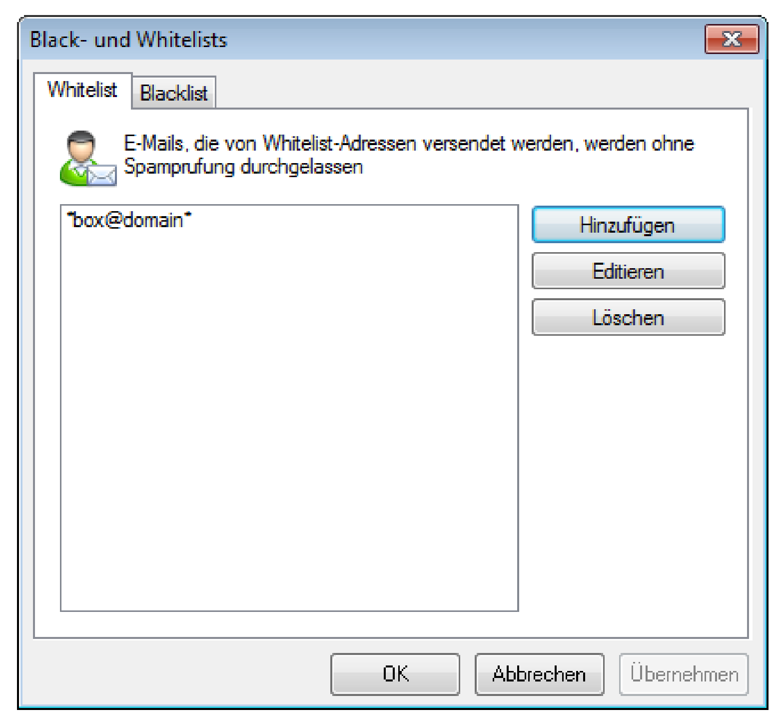


Abbildung 11-4. Einstellungsfenster des Whitelists vom Spam-Filter.

Um eine E-Mail-Adresse zur Black- oder Whitelist hinzuzufügen:

1. Klicken Sie auf **Hinzufügen**.
2. Geben Sie die E-Mail-Adresse im entsprechenden Feld (s. Eingabemethoden für Whitelist und Blacklist).
3. Klicken Sie auf **OK** im Fenster **Liste bearbeiten**.

Um die E-Maiil-Adressen in der Liste zu ändern:

1. Wählen Sie die Adresse in der Liste aus und klicken Sie auf **Ändern**.
2. Bearbeiten Sie erforderliche Informationen.
3. Klicken Sie auf **OK** im Fenster **Liste bearbeiten**.



Um eine E-Mail-Adresse aus der Liste zu entfernen:

1. Wählen Sie die E-Mail-Adresse in der Liste aus.
2. Klicken Sie auf **Löschen**.

Im Fenster **White- und Blacklists** klicken Sie auf **OK**, um Änderungen zu speichern.

Whitelist

Wenn die Absenderadresse der Whitelist hinzugefügt wird, wird die E-Mail auf Spam nicht geprüft. Wenn aber die Domain-Namen der Empfänger- und Absenderadressen gleich sind und dieser Domain-Name in die Whitelist mit der "*" Maske eingetragen ist, so wird die E-Mail auf Spam geprüft.

Eingabemethoden

- um einen bestimmten Absender in die Liste hinzuzufügen, geben Sie seine komplette E-Mail-Adresse (z.B. mail@example.net) an. Alle E-Mails, die von dieser Adresse erhalten werden, werden ohne Spam-Prüfung zugestellt;
- jedes Element der Liste kann nur eine E-Mail-Adresse oder eine Maske enthalten;
- um die E-Mail-Adressen bestimmter Art in die Absenderliste hinzuzufügen, geben Sie eine Maske, die diese Adressen definiert, ein. Die Maske setzt das Template zur Definition des Objektes fest. Sie kann übliche Zeichen, die in E-Mail-Adressen erlaubt sind, sowie das spezielle * Zeichen, mit dem eine beliebige (auch leere) Zeichenfolge ersetzt werden kann, beinhalten.

  Beispielsweise sind folgende Varianten möglich:

  - `mailbox@domain.com`
  - `*box@domain.com`
  - `mailbox@dom*`
  - `*box@dom*`



Das * Zeichen wird nur am Anfang oder am Ende der E-Mail-Adresse gesetzt.

Das @ Zeichen ist obligatorisch.

- um E-Mails von E-Mail-Adressen einer bestimmten Domain garantiert zu erhalten, benutzen Sie das * Zeichen anstatt des Benutzernamens. Um alle E-Mails z.B. von Adressaten auf der `example.net` Domain zu erhalten, geben Sie `*@example.net` ein;
- um E-Mails von E-Mail-Adressen mit einem bestimmten Benutzernamen von einer beliebigen Domain garantiert zu erhalten, benutzen Sie das * Zeichen anstatt des Domain-Namens. Um alle E-Mails z.B. von Adressaten mit dem Namen des E-Mail-Postfaches "ivanov" zu erhalten, geben Sie `ivanov@*` ein.

Blacklist

Wenn die Absenderadresse der Blacklist hinzugefügt wird, wird die E-Mail ohne zusätzliche Analyse als Spam eingestuft.

▸ Eingabemethoden

- um einen bestimmten Absender in die Liste hinzuzufügen, geben Sie seine komplette E-Mail-Adresse (z.B. spam@spam.ru) an. Alle E-Mails, die von dieser Adresse erhalten werden, werden automatisch als Spam eingestuft;
- jedes Element der Liste kann nur eine E-Mail-Adresse oder eine Maske enthalten;
- um die E-Mail-Adressen bestimmter Art in die Absenderliste hinzuzufügen, geben Sie eine Maske, die diese Adressen definiert, ein. Die Maske setzt das Template zur Definition des Objektes fest. Sie kann übliche Zeichen, die in E-Mail-Adressen erlaubt sind, sowie das spezielle * Zeichen, mit dem eine beliebige (auch leere) Zeichenfolge ersetzt werden kann, beinhalten.

  Beispielsweise sind folgende Varianten möglich:

  - `mailbox@domain.com`

- *box@domain.com
- mailbox@dom*
- *box@dom*



Das * Zeichen wird nur am Anfang oder am Ende der E-Mail-Adresse gesetzt.

Das @ Zeichen ist obligatorisch.

- um E-Mails von E-Mail-Adressen einer bestimmten Domain als Spam garantiert zu markieren, benutzen Sie das * Zeichen anstatt des Benutzernamens. Um alle E-Mails z.B. von Adressaten auf der spam.ru Domain als Spam zu markieren, geben Sie *@spam.ru ein;
- um E-Mails von E-Mail-Adressen mit einem bestimmten Benutzernamen von einer beliebigen Domain als Spam garantiert zu markieren, benutzen Sie das * Zeichen anstatt des Domain-Namens. Um alle E-Mails z.B. von Adressaten mit dem Namen des E-Mail-Postfaches "ivanov" als Spam zu markieren, geben Sie ivanov@* ein;
- die E-Mail-Adressen auf Domain des Empfängers werden nicht bearbeitet. Falls die E-Mail-Adresse des Empfängers (Ihre E-Mail-Adresse) beispielsweise auf der mail.ru Domain eingerichtet wurde, so werden die Absenderadressen der mail.ru Domain vom Spam-Filter nicht bearbeitet.

11.3. Protokollieren der Ereignisse

Dr.Web für Outlook registriert Fehler und geschehende Ereignisse in folgenden Logdateien:

- Ereignis-Logdatei des Betriebssystems (Event Log);
- Debug.log Datei.



11.3.1. Ereignis-Log-Datei

In der Ereignis-Log-Datei (Event Log) werden folgende Informationen protokolliert:

- Meldungen beim Starten und Beenden des Programms.
- Parameter der Lizenzschlüsseldatei: Gültigkeit oder Ungültigkeit der Lizenz, Gültigkeitsdauer der Lizenz (Information wird beim Starten des Programms, während des Programmlaufes und beim Ersetzen der Lizenzschlüsseldatei protokolliert).
- Parameter der Programm-Module: Scanner, Engine, Virendatenbanken (Information wird beim Starten des Programms und bei Aktualisierung der Module protokolliert).
- Meldung über Ungültigkeit der Lizenz: keine Freigabe zur Nutzung der Programm-Module in der Lizenzschlüsseldatei, blockierte Lizenz, Integrität der Schlüsseldatei beschädigt (Information wird beim Starten des Programms und während des Programmlaufes protokolliert).
- Meldungen beim Virenfund.
- Benachrichtigungen über Gültigkeitsablauf der Lizenz (Information wird 30, 15, 7, 3, 2 und 1 Tage vor Gültigkeitsablauf protokolliert).

Um die Ereignis-Log-Datei des Betriebssystems anzusehen:

1. Öffnen Sie die **Systemsteuerung**.
2. Wählen Sie **Verwaltung** - **Ereignisanzeige** aus.
3. Im linken Fensterbereich der **Ereignisanzeige** wählen Sie den Menüpunkt **Anwendung** aus. Es öffnet sich die Liste der Ereignisse, die durch Benutzeranwendungen in der Logdatei registriert wurden. Als Informationsquelle für **Dr.Web für Outlook** tritt die Anwendung **Dr.Web for Outlook** auf.



11.3.2. Debug.log Datei

In der Debug.log Datei werden folgende Informationen protokolliert:

- Meldungen über Gültigkeit oder Ungültigkeit der Lizenz.
- Meldungen beim Virenfund.
- Meldungen über Schreib- oder Lesefehler der Dateien, Analysefehler bei Archiven und Dateien, die mit Passwort geschützt sind.
- Parameter der Programm-Module: Scanner, Engine, Virendatenbanken.
- Meldungen über sofortiges Stoppen der Programm-Engine.
- Benachrichtigungen über Gültigkeitsablauf der Lizenz (Information wird 30, 15, 7, 3, 2 und 1 Tage vor Gültigkeitsablauf protokolliert).



Durch die Führung der Debug.log Datei wird die Geschwindigkeit des Betriebssystems beeinträchtigt. In diesem Zusammenhang ist es empfehlenswert, die Protokollierung der Ereignisse nur zu aktivieren, wenn Fehler in der Funktion der **Dr.Web für Outlook** Anwendung auftreten.

Protokollierung der Ereignisse einstellen

1. Im Tab **Dr.Web Antivirus** klicken Sie auf **Protokoll**. Es öffnet sich das Einstellungsfenster der Logdatei.
2. Wählen Sie die Detailtiefe (von 0 bis 5) zum Protokollieren der Ereignisse:
   - Detailtiefe **0** heisst, dass keine Ereignisse in der Debug.log Datei protokolliert werden.
   - Detailtiefe **5** entspricht dem maximalen Detaillierungsgrad der zu protokollierenden Ereignisse.

   Per Default ist das Protokollieren der Ereignisse deaktiviert.
3. Geben Sie die maximale Größe (in Kilobytes) der Logdatei an.
4. Klicken Sie auf **OK**, um Änderungen zu speichern.



Das Fenster **Protokoll** ist nur zugänglich, wenn der Benutzer Systemadministratorrechte besitzt.

Wenn Sie unter Windows Vista und neuer auf **Protokoll** klicken:

- Bei aktivierter UAC: der Administrator erhält eine Aufforderung zur Bestätigung von Programmaktionen. Der Benutzer ohne Administratorrechte erhält eine Aufforderung zur Eingabe von Identifiezierungsdaten des Systemadministrators.
- Bei deaktivierter UAC: der Administrator kann Programmeinstellungen ändern. Der Benutzer erhält keinen Zugriff auf Änderung von Einstellungen.

Ereignis-Logdatei ansehen

Zum Ansehen der Ereignis-Logdatei klicken Sie auf **Im Ordner anzeigen**. Es öffnet sich der Ordner, in dem die Logdatei gespeichert wird.

Standardgemäß wird das Protokoll in der `DrWebOutlook.log` Datei gespeichert. Diese Datei befindet sich im Benutzerprofil des `DoctorWeb` Ordners.



Die Logdatei `DrWebOutlook.log` wird für jeden einzelnen Benutzer des Betriebssystems separat geführt.

11.4. Statistik

Die E-Mail-Anwendung Microsoft Outlook, Abschnitt **Extras** → **Optionen** → Tab **Dr.Web Antivirus** enthält statistische Informationen über die Gesamtanzahl der Objekte, die vom Programm geprüft und bearbeitet wurden.

Die Objekte werden in folgende Kategorien aufgeteilt:

- **Geprüft** - Gesamtanzahl der geprüften E-Mails.



- **Infiziert** - Anzahl der E-Mails, die Viren enthalten.
- **Verdächtig** - Anzahl der E-Mails, die vermutlich mit einem Virus infiziert sind (Ergebnis der heuristischen Analyse).
- **Desinfiziert** - Anzahl der Objekte, die vom Programm erfolgreich desinfiziert wurden.
- **Nicht geprüft** - Anzahl der Objekte, deren Prüfung unmöglich ist oder bei deren Prüfung Fehler aufgetreten sind.
- **Sauber** - Anzahl der E-Mails, die keine schädlichen Objekte enthalten.

Dann wird die Anzahl der Objekte wie folgt angezeigt:

- **In Quarantäne** - Anzahl der Objekte, die in Quarantäne verschoben wurden.
- **Gelöscht** - Anzahl der Objekte, die aus dem System gelöscht wurden.
- **Übersprungen** - Anzahl der Objekte, die ohne Änderungen übersprungen wurden.
- **Spam-Mails** - Anzahl der E-Mails, die als Spam markiert wurden.

Statistikdatei

Standardgemäß wird die Statistik in der `drwebforoutlook.stat` Datei gespeichert, die sich im Benutzerprofil des `DoctorWeb` Ordners befindet. Zur Statistikbereinigung müssen Sie diese Datei löschen.



Die Statistikdatei `drwebforoutlook.stat` wird für jeden einzelnen Benutzer des Betriebssystems separat geführt.

Die Statistiken der **Dr.Web für Outlook** Anwendung werden mit Statistiken sonstiger Antivirus-Komponenten von **Dr.Web Enterprise Security Suite** zusammen dem **Agenten** zum Versand an den **Server** übergeben.



Anhang A. Befehlszeilenschlüssel für Scanner

Während der Scan-Prüfung wird **Dr.Web Scanner** gestartet. Gegebenenfalls können zusätzliche Prüfparameter angegeben werden. Im Eingabefeld **Parameter** können Sie folgende Schlüssel angeben (mit Leerzeichen getrennt):

- /@<*Name der Datei*> oder /@+<*Name der Datei*>

  schreibt vor, dass die Prüfung der in der angegebenen Datei aufgelisteten Objekte ausgeführt wird. Jedes Objekt wird jeweils in einer separaten Zeile der Liste definiert. Dies kann entweder ein kompletter Pfad mit Angabe des Dateinamens oder die Zeile `?boot`, welche die Überprüfung von Bootsektoren bedeutet, sein. Für die GUI-Version des **Scanners** sind es auch Dateinamen mit der Maske und Ordnernamen. Die Listendatei kann manuell mit Hilfe eines beliebigen Texteditors sowie auch automatisch mittels Anwendungen, die den Scanner zur Überprüfung von bestimmten Dateien benutzen, vorbereitet werden. Nach Abschluss der Überprüfung entfernt der Scanner die Listendatei, wenn die Schlüsselform ohne "+" Zeichen benutzt wurde.

- /AL

  alle Dateien auf gegebener Hardware bzw. im gegebenen Ordner prüfen, unabhängig von der Erweiterung bzw. vom internen Format.

- /AR

  Dateien innerhalb von Archiven prüfen. Zur Zeit wird die Überprüfung (ohne Wiederherstellung) von Archiven unterstützt, die durch ARJ, PKZIP, ALZIP, AL RAR, LHA, GZIP, TAR, BZIP2, 7-ZIP, ACE usw. erstellt wurden, sowie von MS CAB-Archiven – Windows Cabinet Files (QUANTUM-Verpackung wird zu diesem Zeitpunkt nicht unterstüzt) und ISO-Images optischer Datenträger (CD und DVD). In der angegebenen Form (/AR) definiert der Schlüssel die Benachrichtigung des Benutzers bei Entdeckung eines Archivs, das infizierte oder verdächtige Dateien

enthält. Wenn der Schlüssel von der Basis-Registry D, M oder R ergänzt wird, werden andere Aktionen ausgeführt:

- /ARD – entfernen;
- /ARM – verschieben (per default - in den Quarantäne-Ordner);
- /ARR – umbenennen (per default wird der erste Buchstabe der Erweiterung durch das "#" Zeichen ersetzt). Der Schlüssel kann mit der Basis-Registry N enden. In diesem Fall wird der Name des Archivers nach dem Namen der Archivdatei nicht angezeigt.

◆ /CU

Aktionen bei infizierten Dateien und Bootsektoren der Festplatten. Ohne zusätzliche Einstellungen D, M oder R wird die Wiederherstellung von desinfizierbaren Objekten und das Entfernen von nicht desinfizierbaren Dateien ausgeführt (falls das Gegenteil durch den Parameter /IC nicht bestimmt wird). Sonstige Aktionen werden nur für infizierte Dateien ausgeführt:

- /CUD – entfernen;
- /CUM – verschieben (per default - in den Quarantäne-Ordner);
- /CUR – umbenennen (per default wird der erste Buchstabe der Erweiterung durch das "#" Zeichen ersetzt).

◆ /SPR, /SPD oder /SPM

Aktionen für verdächtige Dateien:

- /SPR – umbenennen,
- /SPD – entfernen,
- /SPM – verschieben.

◆ /ICR, /ICD oder /ICM

Aktionen für infizierte Dateien, die man nicht wiederherstellen kann:

- /ICR – umbenennen,
- /ICD – entfernen,




- /ICM – verschieben.

◆ /MW

Aktionen für alle Arten der unerwünschten Software. In der angegebenen Form (/MW) bedeutet der Schlüssel die Benachrichtigung des Benutzers. Wird der Schlüssel mit dem Basisregister D, M, R oder I ergänzt, werden sonstige Aktionen ausgeführt:

- /MWD – entfernen;
- /MWM – verschieben (per default - in den Quarantäne-Ordner);
- /MWR – umbenennen (per default wird der erste Buchstabe der Erweiterung durch das "#" Zeichen ersetzt);
- /MWI – ignorieren. Aktionen für bestimmte Arten unerwünschter Software werden mit den Schlüsseln /ADW, /DLS, /JOK, /RSK, /HCK definiert.

◆ /DA

Computer einmal am Tag testen. Das Datum der nächsten Prüfung wird in der Konfigurationsdatei gespeichert, deswegen muss sie zum Erstellen sowie zum nachfolgenden Neuschreiben zugänglich sein.

◆ /EX

Dateien mit Erweiterungen prüfen, die in der Konfigurationsdatei gespeichert sind. Nach Default-Einstellungen oder beim Fehlen der Konfigurationsdatei sind es die Erweiterungen EXE, COM, DLL, SYS, VXD, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, 386, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, PP?, OBJ, LIB, PIF, AR?, ZIP, R??, GZ, Z, TGZ, TAR, TAZ, CAB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SH, SHB, SHS, SHT*, MSG, CHM, XML, PRC, ASP, LSP, MSO, OBD, THE*, EML, NWS, SWF, MPP, TBB.





Wenn ein Element in der Liste der zu prüfenden Objekte eine explizite Angabe der Dateierweiterung enthält, wenn auch mit speziellen * und ? Zeichen, werden nicht nur Dateien mit den zur Liste passenden Erweiterungen, sondern auch alle in dieser Liste angegebenen Dateien geprüft.

- `/FN`

  russische Buchstaben in den Zeichengenerator des Videoadapters laden (nur für **Dr.Web für DOS**).

- `/GO`

  Paketmodus der Programmfunktion. Alle Fragen, die eine Antwort des Benutzers erwarten, werden ignoriert; Beschlüsse, welche eine Auswahl erfordern, werden automatisch gefasst. Es ist empfehlenswert, diesen Modus ist bei der automatischen Prüfung von Dateien, z.B. bei der ganztägigen E-Mail-Prüfung auf dem Server, zu verwenden.

- `/SCP:` <*n*>

  legt die Scanpriorität fest. <*n*> kann die Werte von 1 bis 50 inkl. annehmen.

- `/SHELL`

  gilt für die GUI-Version des Scanners. Unterdrückt das Anzeigen des Startbildes, deaktiviert die Prüfung des Speichers und selbstladender Dateien. Es werden auch die früher gespeicherten Listen mit Pfaden der Dateien und Ordner, die vordefiniert gescannt werden sollen, zur Prüfung nicht geladen. Dieser Modus erlaubt es, die GUI-Version des **Scanners** statt der Konsolen-Version für die Prüfung nur solcher Objekte zu benutzen, die in den Einstellungen der Befehlszeile enthalten sind.

- `/ST`

  definiert den versteckten Funktionsmodus des GUI-**Scanners**. Das Programm funktioniert, indem es keine Fenster öffnet und sich selbst schließt. Sollten aber Viren beim Scannen entdeckt werden, öffnet sich das Standard-Fenster des **Scanners** nach dem Programmablauf. Dieser Modus des **Scanners** setzt voraus,




dass eine Liste der zu prüfenden Objekte in der Befehlszeile definiert wird.

- /HA

  führt die heuristische Analyse von Dateien durch und sucht nach unbekannten Viren darin.

- /INI: *<Pfad>*

  andere Konfigurationsdatei mit dem angegebenen Namen oder Pfad verwenden.

- /NI

  Parameter, die in der drweb32.ini Konfigurationsdatei der Software gespeichert werden, nicht verwenden.

- /LNG: *<Dateiname>* oder /LNG

  alternative Datei der Sprachressourcen (dwl-Datei) mit dem angegebenen Namen oder Pfad verwenden. Falls der Pfad nicht angegeben ist, die integrierte Sprache (English) verwenden.

- /ML

  Dateien überprüfen, die ein E-Mail-Format haben (UUENCODE, XXENCODE, BINHEX und MIME). In der genannten Form (/ML) definiert der Schlüssel die Benachrichtigung des Benutzers bei Entdeckung eines infizierten oder verdächtigen Objektes im E-Mail-Archiv. Wird der Schlüssel mit einem Indexregister D, M, oder R, ergänzt, so werden andere Aktionen ausgeführt:

  - /MLD – entfernen;
  - /MLM – verschieben (per default - in den Quarantäne-Ordner);
  - /MLR – umbenennen (per default wird der erste Buchstabe der Erweiterung durch das "#" Zeichen ersetzt).
  - Der Schlüssel kann auch mit dem zusätzlichen Indexregister N enden (gleichzeitig können auch Basisregister festgesetzt werden). In diesem Fall wird die Anzeige der Information über E-Mail-Dateien deaktiviert.



- `/NS`

  Möglichkeit, die Computerprüfung abzubrechen, verbieten. Nach Angabe dieses Parameters kann der Benutzer die Ausführung des Programms durch Drücken der ESC-Taste nicht abbrechen.

- `/OK`

  komplette Liste von Objekten zum Scannen ausgeben, indem nicht infizierte Objekte mit dem **OK** Vermerk markiert werden.

- `/PF`

  Bestätigung für Prüfung nächster Diskette anfordern.

- `/PR`

  Eine Aufforderung der Bestätigung vor Aktion anzeigen.

- `/QU`

  Scanner prüft die in der Befehlszeile angegebenen Objekte (Dateien, Datenträger, Ordner). Danach wird seine Funktion automatisch beendet (gilt nur für die GUI-Version des **Scanners**).

- `/RP`<*Dateiname*> oder `/RP+`<*Dateiname*>

  Bericht über die Funktionsweise der Software in einer Datei speichern, deren Name im Schlüssel angegeben ist. Ist der Dateiname nicht angegeben, soll der Bericht in einer vordefinierten Datei gespeichert werden. Wenn das Zeichen + vorhanden ist, wird die Datei ergänzt, wenn es fehlt, wird sie neu erstellt.

- `/NR`

  keine Logdatei erstellen.

- `/SD`

  Unterordner prüfen.

- `/SO`

  Tonbegleitung einschalten.

- `/SS`




nach Arbeitsende Modi speichern, die beim aktuellen Start der Software in der Konfigurationsdatei angegeben wurden.

- `/TB`

  Bootsektoren und Haupt-Bootsektoren (MBR) der Festplatte prüfen.

- `/TM`

  nach Viren im Innenspeicher suchen (einschließlich des Windows-Systembereiches, es gilt nur für Windows-**Scanner**).

- `/TS`

  nach Viren in Autorun-Dateien suchen (im `Autorun` Ordner, in systemeigenen `ini`-Dateien, in der Windows-Registry). Es gilt nur für Windows-**Scanner**.

- `/UP` oder `/UPN`

  ausführbare Dateien überprüfen, die mit ASPACK, COMPACK, DIET, EXEPACK, LZEXE usw. verpackt wurden; Dateien, die mit BJFNT, COM2EXE, CONVERT, CRYPTCOM usw. geändert wurden sowie Dateien, die mit CPAV, F-XLOCK, PGPROT, VACCINE usw. immunisiert wurden, prüfen. Damit der Scanner den Namen des Programms, das zum Verpacken, Ändern oder Immunisieren verwendet wurde, nicht anzeigt, wird der Schlüssel `/UPN` verwendet.

- `/WA`

  Programm bis zum Drücken einer beliebigen Schaltfläche nicht beenden, wenn Viren bzw. verdächtige Objekte entdeckt wurden (nur für den Konsolen-**Scanner**).

- `/?`

  kurze Auskunft über Verwendung des Programms anzeigen.

Manche Parameter lassen am Ende das "-" Zeichen verwenden. In solcher "negativen" Form bedeutet es das Deaktivieren des entsprechenden Modus. Solche Option kann dann nützlich sein, wenn dieser Modus nach Default-Einstellungen bzw. nach den in der Konfigurationsdatei früher vorgenommenen Einstellungen aktiviert ist.

Die Liste von Einstellungen der Befehlszeile, die eine "negative" Form zulassen:
/ADW /AR /CU /DLS /FN /HCK /JOK /HA /IC /ML /MW /OK /PF /PR /RSK /SD /SO /SP /SS/TB /TM /TS /UP /WA

Für die Schlüssel /CU, /IC und /SP bricht die "negative" Form die Ausführung beliebiger Aktionen ab, die in der Beschreibung dieser Parameter angegeben sind. Dies bedeutet, dass die Informationen über infizierte und verdächtige Objekte im Protokoll fixiert werden, es werden jedoch keine Aktionen für diese Objekte ausgeführt.

Für die Schlüssel /INI und /RP wird die "negative" Form entsprechend als /NI und /NR geschrieben.

Für die Schlüssel /AL und /EX ist keine "negative" Form vorgesehen. Das Definieren von einem Schlüssel macht die Aktion des anderen ungültig.

Wenn mehrere inkompatible Schlüssel in der Befehlszeile verwendet werden, so ist dann der letzte Schlüssel gültig.



Anhang B. Vollständige Liste von unterstützten Betriebssystemen

Betriebssysteme der UNIX-Familie:

Linux glibc 2.7 und höher
FreeBSD 7.3 und höher
Sun Solaris 10 (nur für Intel-Plattform)

Windows Betriebssysteme:

- 32 bit:

Windows 98
Windows Millennium Edition
Windows NT4 (SP6a)
Windows 2000 Professional (SP4 auch mit Update Rollup 1)
Windows 2000 Server (SP4 auch mit Update Rollup 1)
Windows XP Professional (auch mit SP1 und höher)
Windows XP Home (auch mit SP1 und höher)
Windows Server 2003 (auch mit SP1 und höher)
Windows Vista (auch mit SP1 und höher)
Windows Server 2008 (auch mit SP1 und höher)
Windows 7

- 64 bit:

Windows Server 2003 (auch mit SP1 und höher)
Windows Vista (auch mit SP1 und höher)
Windows Server 2008 (auch mit SP1 und höher)
Windows Server 2008 R2
Windows 7



SelfPROtect, SpIDer Gate, Office Kontrolle, FireWall

- 32 bit:

Windows 2000 Professional (SP4 auch mit Update Rollup 1)
Windows 2000 Server (SP4 auch mit Update Rollup 1)
Windows XP Professional (auch mit SP1 und höher)
Windows XP Home (auch mit SP1 und höher)
Windows Server 2003 (auch mit SP1 und höher)
Windows Vista (auch mit SP1 und höher)
Windows Server 2008 (auch mit SP1 und höher)
Windows 7

- 64 bit:

Windows Server 2003 (auch mit SP1 und höher)
Windows Vista (auch mit SP1 und höher)
Windows Server 2008 (auch mit SP1 und höher)
Windows Server 2008 R2
Windows 7

Windows Mobile

Windows Mobile 2003
Windows Mobile 2003 Second Edition
Windows Mobile 5.0
Windows Mobile 6.0
Windows Mobile 6.1

Novell NetWare

Novell NetWare 3.12
Novell NetWare 3.2
Novell NetWare 4.11
Novell NetWare 4.2

Novell NetWare 5.1

Novell NetWare 6.0

Novell NetWare 6.5

Mac OS X

Mac OS 10.4 (Tiger)
Mac OS 10.4 Server (Tiger Server)
Mac OS 10.5 (Leopard)
Mac OS 10.5 Server (Leopard Server)
Mac OS 10.6 (Snow Leopard)
Mac OS 10.6 Server (Snow Leopard Server)



Die Beschreibung von Funktionalität des **Ageneten** unter Windows Mobile und Novel NetWare finden Sie in Benutzerhandbüchern **Dr.Web Agent für Windows Mobile** und **Dr.Web Agent für Novell NetWare**.



Anhang C. Entdeckungsverfahren von Viren

Alle Antivirus-Komponenten von **Dr.Web** setzen gleichzeitig mehrere Entdeckungsverfahren von schädlichen Objekten ein. Dies ermöglicht, maximal sorgfältig alle verdächtigen Dateien zu prüfen und das Verhalten der Software zu kontrollieren:

1. In erster Linie wird die Signaturanalyse eingesetzt. Dieses Verfahren lässt den Code von verdächtigen Dateien analysieren, um festzustellen, ob sie den bekannten Virensignaturen entsprechen (Signatur ist eine kontinuerliche endliche Byte-Reihnfolge, die für Erkennung eines Virus erforderlich und ausreichend ist). Dabei werden die Prüfsummen von Signaturen verglichen, was zu einer wesentlichen Verringerung der Virendatenbankgröße beiträgt. Dabei bleibt die eindeutige Übereinstimmung und demgemäß die Zuverlässigkeit bei Virusentdeckung und Desinfizierung der verdächtigen Dateien erhalten. Die **Dr.Web Virendatenbanken** sind so zusammengesetzt, dass nur mit einer Signatur mehrere Klassen von Bedrohungen entdeckt werden können.
2. Nach der Signaturanalyse wird die einzigartige Origins Tracing™ Technologie eingesetzt, die zur Entdeckung von neuen und modifizierten Viren dient, die bekannte Infizierungsmechanismen benutzen. Dieses Verfahren schützt die Benutzer von **Dr.Web** Antivirus-Lösungen vor solchen Viren, wie z.B. Erpresservirus Trojan.Encoder.18 (das auch unter dem Namen gpcode bekannt ist). Weiterhin lässt **Origins Tracing** die Anzahl von Fehlauslösungen der heuristischen Analyse reduzieren.
3. Das Prinzip der heuristischen Analyse basiert auf Wissen (Heuristiken) über kennzeichnende Merkmale eines Viruscodes sowie eines zuverlässigen Codes. Jedes Merkmal besitzt bestimmten Wert (eine Zahl, die Wesentlichkeit und Zuverlässigkeit dieses Merkmales anzeigt). Aufgrund des Gesamtwertes, der jede bestimmte Datei definiert, wird die Wahrscheinlichkeit von Datei-Infizierung mit einem



unbekannten Virus mittels der heuristischen Analyse festgestellt. Wie auch jedes System der Hypothesenprüfung unter Unbestimmtheitsbedingungen kann die heuristische Analyse Fehler der ersten (Nichterkennung der unbekannten Viren) sowie der zweiten Art (Falschmeldung) bringen.

Bei einer beliebigen Prüfung werden die aktuellsten Informationen über bekannte Schadprogramme von Dr.Web Antivirus-Komponenten verwendet. Die Virensignaturen, Infos über ihre Merkmale und Verhaltensmodelle werden sofort aktualisiert, wenn Experten aus dem **Virenlabor von Doctor Web** neue Bedrohungen entdecken, manchmal kann es mehrmals pro Stunde passieren. Regelmäßige Aktualisierung der Virendatenbanken lässt auch die neuesten Viren entdecken.



Schlagwortregister



Schlagwortregister



Schlagwortregister



Schlagwortregister